VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2021 Karolína Obdržálková

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

METODY STEGANOGRAFIE
METHODS OF STEGANOGRAPHY

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Karolína Obdržálková**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Vlastimil Člupek, Ph.D.**
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Studentka: Karolína Obdržálková ***ID:*** 211324

Ročník: 3 ***Akademický rok:*** 2020/21

NÁZEV TÉMATU:

Metody steganografie

POKYNY PRO VYPRACOVÁNÍ:

V bakalářské práci proveďte analýzu současných metod steganografie. Popište možnosti využití steganografie při ochraně děl podle autorských práv a při šíření škodlivého softwaru. Na základě provedené analýzy navrhněte multiplatformní aplikaci využívající zvolenou metodu steganografie ke skrytí a odhalení informace. Aplikace bude umět volitelně zajistit integritu, autentičnost a důvěrnost skryté informace. Implementujte Vámi navrženou aplikaci, ověřte její funkčnost, přehledně prezentujte její možnosti použití a ohodnoťte úroveň zabezpečení skryté informace pomocí Vámi navržené aplikace.

DOPORUČENÁ LITERATURA:

[1] ZIELIŃSKA, Elżbieta; MAZURCZYK, Wojciech; SZCZYPIORSKI, Krzysztof. Trends in steganography. Communications of the ACM, 2014, 57.3: 86-95.

[2] ANDERSON, Ross J.; PETITCOLAS, Fabien AP. On the limits of steganography. IEEE Journal on selected areas in communications, 1998, 16.4: 474-481.

Termín zadání: 1.2.2021 ***Termín odevzdání:*** 31.5.2021

Vedoucí práce: Ing. Vlastimil Člupek, Ph.D.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

UPOZORNĚNÍ:
Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

ABSTRAKT

Tato bakalářská práce se zabývá steganografií, jejími druhy a metodami. V rámci této práce je obecně popsána steganografie. Značná část je věnována vývoji steganografie a možnostem využití této bezpečnostní disciplíny při šíření škodlivého softwaru a při ochraně autorských děl. V další části jsou popsány druhy steganografie rozdělené podle nosiče, jejich metody a také vlastnosti steganografických metod. Na základě teoretických poznatků byla vytvořena aplikace s grafickým uživatelským rozhraním umožňující skrytí a odhalení tajné informace s využitím steganografické metody LSB. Tato aplikace je popsána v závěrečné části spolu s ohodnocením úrovně zabezpečení skrývaných informací.

KLÍČOVÁ SLOVA

AES, bezpečnost, historie, HMAC, kapacita, LSB, nepostřehnutelnost, robustnost, steganografie, škodlivý software, vodoznaky

ABSTRACT

This bachelor thesis deals with steganography, its types and methods. Steganography is generally described in this work. A significant part of this thesis is devoted to the development of steganography and also describes how is steganography used for malware and copyright protection. The next part describes the types of steganography according to the type of carrier, their methods and properties of steganographic methods. Based on theoretical knowledge, an application with a graphical user interface was created to hide and reveal secret information using steganographic method LSB. This application is described in the final part together with the evaluation of the level of security of hidden information.

KEYWORDS

AES, capacity, history, HMAC, imperceptibility, LSB, malware, robustness, security, steganography, watermarks

Vysázeno pomocí balíčku `thesis` verze 4.03; `http://latex.feec.vutbr.cz`

OBDRŽÁLKOVÁ, Karolína. *Metody steganografie*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2021, 56 s. Bakalářská práce. Vedoucí práce: Ing. Vlastimil Člupek, Ph.D.

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Karolína Obdržálková
VUT ID autora:	211324
Typ práce:	Bakalářská práce
Akademický rok:	2020/21
Téma závěrečné práce:	Metody steganografie

Prohlašuji, že svou závěrečnou práci jsem vypracovala samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autorka uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědoma následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autorky*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Ráda bych poděkovala vedoucímu bakalářské práce panu Ing. Vlastimilu Člupkovi, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Seznam obrázků

Úvod

Tato doba jde, co se týče technického pokroku, stále dopředu. Vyvíjí se nesmírně rychle a je nutné se takovýmto podmínkám přizpůsobovat. Současná technika umožňuje komunikaci na dálku či uchovávání enormního množství osobních dat. Je proto důležité věnovat se způsobům, které zaručí bezpečný přenos předávaných informací nebo ochranu citlivých informací, ať už se jedná o anonymitu, utajení a zašifrování dat či ochranu autorských děl.

Bezpečnostní techniky sloužící k těmto účelům jsou kryptografie, steganografie a s ní dosti blízké vodoznaky.

Steganografie může být popsána jako umění ukrývání tajných informací. Tyto informace totiž dokáže pomocí daných metod ukrýt například do digitálních souborů.

Jedním z cílů této práce je zanalyzovat současné metody steganografie. Existuje velké množství těchto metod. Některé z nich využívají pro skrytí tajných dat obrázku jako nosiče, jiné používají zvukový, textový nebo také video soubor. Dalším cílem je popsat možnosti využití steganografie při ochraně děl podle autorských práv a při šíření škodlivého softwaru. Poté je úkolem vytvořit aplikaci využívající vybranou metodu pro ukrytí a odkrytí tajné zprávy s možností zašifrování.

Kapitola 1 se věnuje popisu steganografie jako vědní disciplíny. Jsou zde vysvětleny základní principy nutné pro hlubší pochopení této problematiky. Tato část se také zabývá porovnáním metod, které se stejně jako steganografie, věnují ochraně dat.

V kapitole 2 jsou popsány nejdůležitější okamžiky v historii, které se zasloužily o vývoj steganografie. S nástupem počítačů a internetu se steganografie přesunula do světa nul a jedniček, a proto se velká část této kapitoly věnuje využití této disciplíny ve 21. století. Steganografie je v téhle době využívána opravdu často, bohužel ale z velké části pro nelegální účely, což je v této kapitole také popsáno. Poslední část se věnuje použití steganografie při ochraně autorských děl.

Kapitola 3 na začátku popisuje důležité vlastnosti steganografických metod, podle kterých se poté určuje zabezpečení skrývané informace. V dalších částech je věnována popisu nejznámějších typů steganografie: obrazové, zvukové a textové steganografii a jejich příslušným metodám.

Kapitola 4 je věnována popisu vytvořené aplikace využívající metodu LSB.

V poslední kapitole 5 je zhodnoceno zabezpečení skrývaných informací pomocí vytvořené aplikace.

1 Steganografie

V této kapitole jsou popsány základní principy steganografie, které je potřeba chápat k hlubšímu porozumění tohoto textu. Podkapitola 1.1 je jakýmsi úvodem do problematiky steganografie. Popisuje samotný význam slova steganografie a co si vůbec pod tímto pojmem představit. V podkapitole 1.2 jsou se steganografií porovnány její velice blízké disciplíny, a to vodoznaky a kryptografie. V následující podkapitole 1.3 je na příkladu Problém věznů jednoduše vysvětlen princip steganografie. Poslední podkapitola 1.4 je věnována vysvětlení základních pojmů, které budou v této práci ve spojitosti s funkcionalitou steganografie používány.

1.1 Steganografie

Steganografie je umění či vědní disciplína s velmi dlouhou existencí, jež má za úkol ukrytí informace (zprávy, dat) tak, aby její existence nebyla vůbec detekována. Zahrnuje velkou škálu komunikačních metod zakrývajících přítomnost tajné zprávy. Mezi ně patří například neviditelné inkousty, mikrotečky, metoda nejméně významného bitu nebo u zvukových souborů ukrývání ozvěny [1]. Díky velkému rozmachu techniky se v současné době steganografie využívá nejčastěji v digitální podobě. V této podobě nám umožňuje skrytí velké škály souborů (tajných dat) různých typů do jiných, tzv. nosičů.

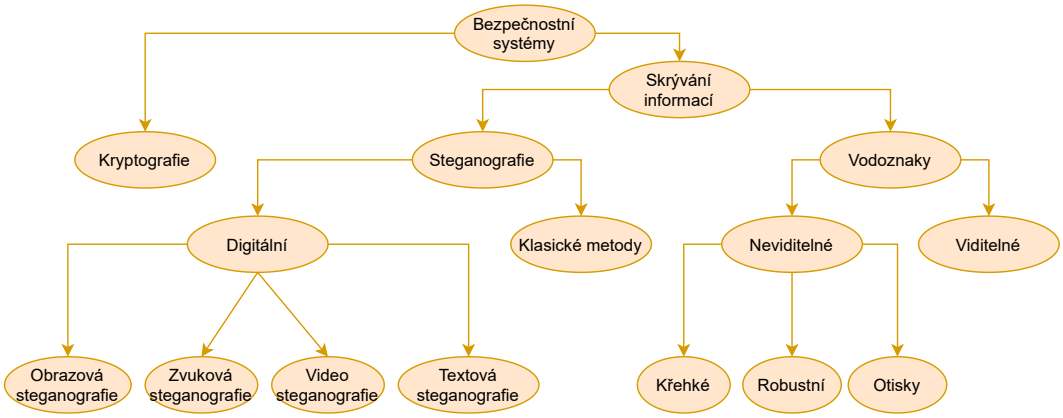
Samotný pojem steganografie vychází z řeckých slov „stegos“ znamenající „skrytý“ a „grafia“ znamenající „psaní“, což dohromady dává spojení „skryté psaní – covered writing“ [2].

1.2 Porovnání s blízkými disciplínami

Velmi blízko ke steganografii mají vodoznaky a kryptografie. Všechny tyto disciplíny se věnují ochraně dat. Existují mezi nimi rozdíly, i když mezi steganografií a vodoznaky je jen velmi tenká hranice, která podle některých zdrojů téměř neexistuje (pokud se jedná o neviditelné vodoznaky) [3]. Jejich hiearchie je ukázána na obrázku 1.1.

Kryptografie zašifruje zprávu tak, že ji poté není bez příslušného klíče možné rozšifrovat. Informace je tedy viditelná, ale nečitelná.

Vodoznaky umožňují vložení dodatečné informace do daného digitálního souboru (často chráněného autorským právem), aby bylo zřejmé, komu soubor patří. Není zde vždy nutné, aby dodatečná informace byla skryta jako je tomu u steganografie, a proto je některými autory vodoznak považován za odlišnou vědní disciplínu. Ne



Obr. 1.1: Hiearchie jednotlivých bezpečnostních disciplín [4].

všichni s tímto rozdělením souhlasí, je tedy možné i odlišné rozdělení, kdy je vodoznak brán jako součást steganografie, už z toho důvodu, že se při jeho implementaci využívá steganografických technik [3, 5].

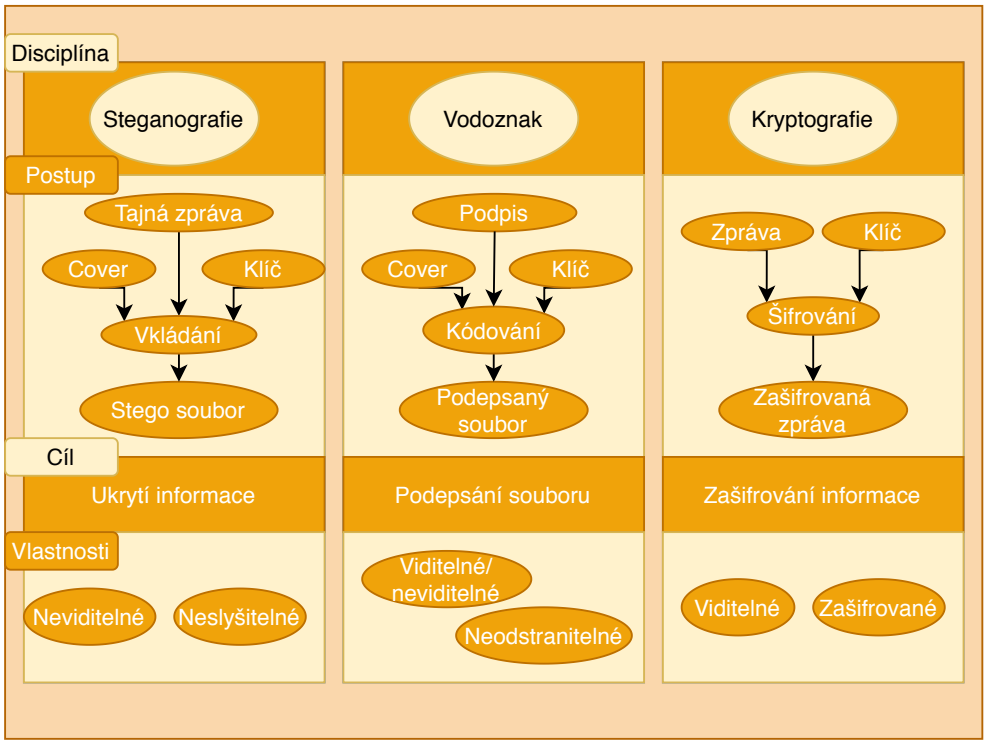
Steganografie tajnou informaci skryje takovým způsobem, abychom o její existenci nevěděli. To je velmi výhodné už z toho důvodu, že zašifrovaná viditelná zpráva může vzbudit podezření, ale pokud je navíc ukryta, tak je tomu naopak. Proto se pro lepší zabezpečení často steganografie kombinuje s kryptografickými technikami. V případě, že by tajná informace byla i přes ukrytí objevena, by zde ještě byla dodatečná ochrana v podobě kryptografického zašifrování [2]. Rozdíl mezi těmito třemi disciplínami je názorně ukázán na obrázku 1.2.

1.3 Problém vězňů

Pro vysvětlení základního principu steganografie se často používá Simmonsův problém vězňů.

Alice a Bob jsou dvě fiktivní postavy, které byly zatčeny a následně umístěny do odlišných cel. Jejich cílem je samozřejmě utéct a dostat se na svobodu. Jediný problém ale je, že mohou komunikovat pouze přes jejich dozorkyni Wendy. Ta je velmi všímavá, pokud by se mezi sebou domlouvaly šifrovaně, všimla by si toho a poslala by je na samotku. Jejich jediným řešením je tedy spolu komunikovat nenápadně, aby nevzbudily podezření. K takovéto komunikaci proto použijí steganografii.

Příklad pokračuje vysvětlením, že nejlepší cestou, jak tohoto docílit, je schovat tajnou zprávu do nenápadně působícího textu nebo do obrázku. Bob by mohl například nakreslit obrázek modré krávy na zelené pastvině a předat jej Wendy, která by se na něj samozřejmě podívala, ale protože by na ni tento obrázek působil pouze jako nějaké abstraktní dílo, předala by jej dál. Netušila by přitom, že barvy na obrázku



Obr. 1.2: Rozdíly mezi jednotlivými disciplínami [6].

předávají tajnou zprávu.

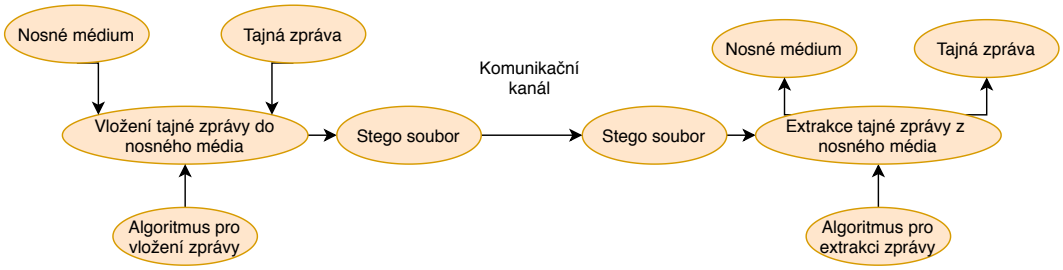
Takovéto řešení samozřejmě může mít slabiny. Wendy by mohla obrázek pozměnit, buďto omylem nebo naschvál, čímž by zprávu změnila nebo zničila. Pokud by obrázek změnila schválně, jednalo by se o aktivní útok. Kdybychom toto více rozvedli, můžeme říct, že by Wendy mohla vytvořit vlastní zprávu a tu podstrčit jednomu z vězňů, který by netušil, že se nejedná o původní zprávu. V tomto případě by šlo o škodlivý útok.

Model problému vězňů lze uplatnit pro mnoho situací, kde může být pro komunikaci užita steganografie. Alice a Bob jsou dvě strany, které spolu chtějí komunikovat a Wendy je slídil. Jde o efektivní způsob komunikace, ale i přes to musejí být vždycky brány v potaz různé pasivní, aktivní či škodlivé útoky [5].

1.4 Základní princip

Princip procesu steganografie je naznačen na obrázku 1.3. Pro jeho pochopení je nutné si sjednotit význam následujících pojmů:

- **zpráva, tajná zpráva, tajná data, tajná informace** – tímto pojmem jsou označena ta data, která jsou určena k ukrytí;



Obr. 1.3: Proces steganografie [7].

- **cover, nosič (nosné médium, nosný soubor), krycí médium** – jde o médium, do kterého jsou ukryta tajná data;
- **stego soubor, stegomédium, steganogram** – jedná se nosič již skrývající tajná data.

Tato disciplína tedy umožňuje lidem tajně komunikovat ukrytím zprávy do krycího média. Odesílatel příjemci pošle tajnou informaci, kterou schová do jiného souboru. Tento soubor může být například ve formátu textu, videa, obrázku nebo zvuku. Tajná data jsou vložena do coveru použitím vhodného algoritmu a tímto procesem následně vznikne stego soubor, který je poslán příjemci.

2 Vývoj a možnosti využití steganografie

Tato kapitola zprostředkovává informace o vývoji steganografie od samého počátku, který se datuje od 5. století až k současným moderním využitím metod této disciplíny. V podkapitole 2.1 je popsáno její používání nejen ve starověkém Řecku nebo Číně, ale i ve středověkém Německu či novověké Itálii. Dozvíme se, komu vděčíme za název samotné disciplíny. Na konci této podkapitoly je popsáno, jak byla steganografie využita během Americké revoluce a následně i během obou světových válek. Podkapitola 2.2 je věnována modernímu využití steganografie, která díky digitální revoluci přešla do světa nul a jedniček. Poslední dvě podkapitoly 2.3 a 2.4 popisují možnosti využití steganografie při šíření škodlivého softwaru a při ochraně autorských děl.

2.1 Historie

Steganografické techniky jsou používány už po staletí. První zmínky jsou již z 5. století ze starověkého Řecka. Zdokumentoval je řecký historik Hérodotos ve svém díle „Dějiny“. Řek Demaratus využil pro předání tajné zprávy voskové psací destičky, ze kterých seškrábal vosk, na dřevěný podklad vyryl vzkaz a následně destičku opět překryl voskem. Tyto tabulky se jevily jako prázdné, a proto mohly být bez povšimnutí poslány dál. Jiným příkladem může být způsob Řeka Histaea, který napsal tajnou zprávu na oholenou hlavu svého otroka a poté, co mu dorostly vlasy, ho vyslal zprávu předat [8].

Ve starověké Číně využívali hedvábí, na které napsali vzkaz. Tento kousek hedvábí následně zmuchlali a obalili voskem. Voskovou kuličku poté spolknul posel a vydal se na cestu. O způsobu předání zprávy se můžeme jen domnívat [9].

O základy pro další rozvoj v oblasti steganografie se zasloužil opat Johannes Trithemius, jehož trojdílný cyklus „“Steganographia“ z roku 1499 popisoval rozsáhlý systém ukrývání tajných zpráv do nevinně vyhlížejících textů a díky kterému se pro tyto techniky začal používat název Steganografie [5].

Zajímavou techniku ukrývání vzkazů vymyslel v 16. století italský vědec Giovanni Porta. Pomocí speciálně vytvořeného roztoku napsal vzkaz na skořápku uvařeného vejce a poté, co vejce tuto tekutinu vstřebalo, nebylo na něm nic znát. Zprávu bylo možné přečíst po oloupání vejce, díky pórovité struktuře skořápky [5].

Další používanou technikou je neviditelný inkoust. Velmi využívaný pro komunikaci byl během americké revoluce oběma stranami. Britové používali dva různé typy inkoustu. První z nich se objevil, pokud byl vystaven teplu. Druhý, pokud byl vystaven kyselině. Georgi Washingtonu toto nestačilo. Chtěl speciální inkoust, aby bylo těžší ho odhalit. James Jay, doktor a bratr amerického congressmana Johna Jay,

vyvinul takzvaný „sympatický inkoust“, který po nanesení na papír zmizel a tajná zpráva se nezobrazila pokud nebylo použito konkrétní odpovídající činidlo. Washington nařídil používání tohoto inkoustu svým agentům. Tajné informace mohly být psány doslova mezi řádky nevinného textu a nikdo, kdo si tohoto tajného způsobu předávání informací nebyl vědom, nic nepoznal [10, 11].

Ve 20. století byly neviditelné inkousty také velmi rozšířené. Během druhé světové války lidé používali k napsání tajných vzkazů mléko, ocet, šťávy z ovoce, ale i moč. Tyto tekutiny totiž, pokud byly zahřány, ztmavly, a proto mohly být následně přečteny [8].

Další používanou praktikou byly nulové šifry [8]. Tajný vzkaz byl schován po písmenech do nevinně vyhlížejícího textu. K dekódování bylo potřeba přečíst n-té písmeno každého slova ve zprávě. Dohromady tato písmena dávala tajnou zprávu. Jedním z příkladu může být následující zpráva, která byla poslaná německých špehem v druhé světové válce: *„Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.“* Přečtením druhého písmena každého slova této zprávy získáme následující vzkaz: *„Pershing sails from NY June I.“*

Němci během druhé světové války vyvinuli a používali techniku zvanou mikrotečky. J. Edgar Hoover nazval tuto techniku „nepřátelským mistrovským dílem špionáže“. Šlo o detailní fotografie, které byly zmenšené do velikosti tečky v textu. Mohlo jít o celé stránky tajného textu nebo fotografie například nějaké vojenské základny. Takovéto miniaturní informace byly vytištěny na filmový podklad a následně nalepeny přes interpunkční znaménka do novin, magazínů nebo dopisů. K přečtení této zprávy bylo nutné použít mikroskop. Rozdíl v lesklosti filmového podkladu a matného papíru dopisů (či novin) prozradil existenci těchto tajných informací [8].

2.2 Moderní steganografie

Mimo předešle zmíněné případy užití steganografických metod v historii můžeme v posledních dvou dekádách pozorovat intenzivní výzkumné úsilí související se steganografií a stegoanalýzou. Tento rychlý vývoj mohl být zčásti způsoben průmyslovým a obchodním zájmem týkajícím se Správy digitálních práv (Digital Rights Management), ve které jsou k ochraně informací a skrytí tajných dat používány steganografické techniky a vodoznaky [12].

S nárustem výkonu počítačů, internetu a rozvoje digitálního zpracování signálu, teorie informace a teorie kódování se takto steganografie přesunula do světa jedniček a nul. Kyberkriminalita z této digitální revoluce těží, jak si ukážeme na následujících příkladech [4].

Významných okamžikem, který mohl vést k dalšímu zkoumání a vývoji steganografických metod, byl teroristický útok na USA z 11. září 2001 při jehož plánování bylo údajně využito steganografie. Objevila se totiž tvrzení, která naznačovala, že pro plánování těchto útoků bylo využito obrazové steganografie a následně byly tyto obrázky s tajnými informacemi zveřejněny na veřejně dostupných webových stránkách. K této utajené komunikaci mělo docházet po dobu tří let. Na Michiganské univerzitě proto prozkoumali přibližně tři miliony obrázků z populárních webových stránek a hledali důkazy, že bylo steganografie opravdu využito. Žádný důkaz ale nenašli [4, 12].

V počátcích digitální steganografie byly vyvíjeny techniky obrazové steganografie. Tato disciplína ze začátku ale kromě digitálních obrázků nepodporovala ke vkládání tajných dat používání komplikovanějších krycích médií jako jsou zvukové či video soubory, VoIP, HTML, spustitelné soubory .exe, XML nebo síťové protokoly [4].

Popularita obrazové steganografie v určitých soukromých sociálních kruzích prudce vzrostla a netrvalo dlouho, než začali zločinci používat tuto formu steganografie k obchodování s nelegálním obsahem přes temný web (dark web). Temný web je část World Wide Webu, která je umístěna na darknetech, tj. překryvných sítích. Ty využívají internet. Pro přístup je nutný speciální software. Vyhledávače temný web neindexují [13].

Technologie jako jsou cenově dostupné počítače, videokamery, anonymní prohlížeče (např. Tor, I2P atd.) a vysokorychlostní internet nesmírně komplikují orgánům činným v trestním řízení bojovat s šířením dětské pornografie online. V roce 2002 vyvrcholila akce zvaná Operation Twins zadržením zločinců z mezinárodní pedofilní organizace Shadowz Brotherhood, která byla zodpovědná za distribuci a obchodování s dětskou pornografií na temném webu. K úkrývání a přenášení nelegálního obsahu totiž využili steganografie, díky které skrývali nelegální obsah do nenápadně vyhlížejících obrázků [12].

Narůstající počet těchto nelegálních událostí zneužívajících steganografie měl za následek oficiální uznání tohoto problému. Roku 2006 byla steganografie jmenována jako jedna z největších hrozeb současných počítačových sítí, u jejíhož zneužívání je předpokládán nárůst. Digitální steganografie je převážně zneužívána crackery, vývojáři malwaru, teroristickými skupinami, zaměstnanci zneužívajících svých pozicí a pedofily. Jedním z možných řešení boje s tímto zneužíváním je seznámit se s vývojem steganografie a následně predikovat další vývoj. Akademický svět tuto potřebu řešení uznal v 80. letech, v této době totiž začala steganografie nabírat na popularitě [12].

Ukázalo se také, že steganografie může sloužit k propašování citlivých informací. Například roku 2008 došlo k úniku citlivých finančních dat z Ministerstva spravedl-

nosti USA, za který byl odpovědný jejich zaměstnanec. Tato data totiž byla ukryta do JPEG obrázků a následně z Ministerstva propašována. USA zažila v minulých letech řadu významných špionážních incidentů, které vedly k úniku velkého množství vysoce utajovaných informací na temný web nebo na webové stránky jako například WikiLeaks [12].

V roce 2010 došlo k odhalení ruského špionážního kruhu takzvaných Illegals, kteří vynášeli vysoce utajované informace z USA do Moskvy. Tito špehové ke komunikaci využívali obrazové steganografie, díky které byli schopni ukrývat instrukce a informace do nevinně vypadajících obrázků na veřejně dostupných webových stránkách [12].

Protože se technika vyvíjí bleskovým tempem, je snadné si vyvodit, že nosič, do kterého jsou vložena tajná data, nemusí být nutně obrázek nebo zdrojový kód webové stránky, ale i jakýkoliv jiný typ souboru, paket nebo rámec, které se v počítačových sítích přirozeně vyskytují.

Steganografické techniky poskytují prostředky pro tajnou komunikaci. Účel těchto technik může být různý, ať už legální či nelegální. Často se zdůrazňuje nelegální aspekt steganografie – počínajíc zjevnou kriminální komunikací, přes úniky tajných informací, výměnu kybernetických zbraní až po průmyslovou špionáž. Na druhé straně ale leží legitimní použití, mezi něž patří obcházení webové cenzury a dohledu, digitální forenzní analýza (sledování a identifikace) a ochrana autorských práv [12].

2.3 Možnosti využití při šíření škodlivého softwaru

Velké oblibě čelí steganografie u crackerů. Nejvíce se využívá obrazové steganografie. Útočníci často využívají legitimních služeb jako jsou bezplatné služby hostování obrázků, což jim slouží k rozšíření těchto souborů mezi velkou část uživatelů. Obrázky mohou rovnou ukrývat payload nebo kód, který se k payloadu určitým způsobem dostane.

K velkému narušení kyberbezpečnosti došlo v roce 2011, které lze připsat tzv. Operaci Shady RAT. Tyto útoky byly zaměřeny na řadu institucí po celém světě a v mnoha případech trvalo měsíce než byly způsobené škody opraveny.

Útok byl prováděn skrze podvodné phishingové emaily s přílohami, po jejichž otevření bylo zařízení oběti infikováno trojským koněm. Dalším krokem bylo připojení k webové stránce a stažení souborů, které působily jako legitimní HTML nebo JPEG soubory. Doopravdy šlo ale o zakódované příkazy vložené do těchto souborů, které díky své nenápadnosti mohly být propašovány přes firewall do napadeného systému. Pomocí těchto řídících příkazů byl infikovaný systém připojen ke vzdáleným serverům a tím získali útočníci přístup k lokálním souborům oběti.

V mnoha případech toto spojení trvalo celé měsíce, což se považuje za velmi závažné narušení bezpečnosti. Útočníci byli tak drzí, že se ani nesnažili skrýt fakt, že pro útok využili steganografie. Jeden z obrázků, do kterého byly řídící příkazy vloženy, byl obrázek 2.1, oříznutý obrázek modelky z časopisu Playboy, což je standardní testovací obrázek, který je využíván pro steganografické testování. Během

Obr. 2.1: Obrázek Lena, který je často využíván pro steganografické testování [14].

tohoto období došlo ještě k několika útokům využívajících steganografii. Objeven byl například počítačový červ zvaný Stuxnet, který byl zaměřen na íránské jaderné elektrárny.

Červu Stuxnet byl podobný červ zvaný Duqu objevený v září 2011. Struktura obou těchto druhů škodlivého softwaru byla stejná. Například funkcionalita počítačového červa Duqu spočívala v přenosu získaných tajných dat skrytých v obyčejných obrázcích k řídícím centrům útočníků, při kterém procházely tyto obrázky absolutně nepovšimnuty [12].

Dalším známým případem zneužití steganografie při šíření škodlivého softwaru je exploit kit Stegano, který byl zpozorován už v roce 2014. Na miliony čtenářů navštěvujících oblíbené zpravodajské weby se zaměřila falešná reklamní kampaň. Šlo o reklamní kampaň na produkty Browser Defence nebo Broxu.

Při návštěvě webu, který danou reklamu obsahoval, byly bez jakékoli interakce s uživatelem zjištěny údaje o jeho prohlížeči a poslány na vzdálený server. Pokud se jednalo o Internet Explorer, byla uživateli místo pravého banneru poslána upravená verze, která nebyla od originálu pouhým okem rozeznatelná.

Upravená verze banneru měla v alfa kanálu (v RGBA modelu alfa kanál určuje průhlednost konkrétního pixelu) zakódovaný skript. Rozdíl oproti originálu byl velmi malý, barevný tón upraveného obrázku se lišil jen mírně.

Skript poté využil známé zranitelnosti Internet Exploreru CVE-2016-0162 a pokusil se ověřit, zda neběží uvnitř monitorovaného prostředí. Pokud nezjistil nic po-

dezřelého, přesměroval se na tzv. Stegano exploit landing stránku prostřednictvím služby TinyURL. Z této stránky načetl flash soubor, který byl schopný využít tří zranitelností Adobe Flash přehrávače (CVE-2015–8641, CVE-2016–1019 a CVE-2016–4117).

Po úspěšném zneužití byl spuštěný kód schopný shromáždit informace o nainstalovaných bezpečnostních produktech a opět si ověřit, že není monitorován. Následně ze stejné stránky stáhl GIF obrázek, ze kterého získal zašifrovaný payload. Payload byl poté dešifrován a spuštěn pomocí regsvr32.exe nebo rundll32.exe. Detekované payloady zahrnovaly trojské koně zaměřené na bankovnictví, spyware nebo backdoory [15, 16].

Útoky často míří na vládní subjekty, diplomaty či telekomunikační operátory, ale nevyhýbají se ani například průmyslovým subjektům. K nedávno objeveným útokům patří kybernetická špionáž odkryta společností Kaspersky, která cílí na průmyslové holdingy a probíhá již od roku 2018 pomocí malwaru MontysThree, který využívá různých technik, aby se zabránilo detekci, včetně hostování komunikace s řídícím serverem na veřejných cloudových službách. K ukrytí hlavního škodlivého modulu je využito právě techniky steganografie.

Funguje pomocí čtyř modulů. První (zavaděč) se zpočátku šíří použitím archivů RAR SFX (archivy schopné sebeextrakce), pomocí spear-phishingových mailů mířících na vybrané firmy, které se snaží oklamat zaměstnance, aby dané přílohy s těmito archivy stáhli. Archivy obsahují PE soubory vydávající se za PDF nebo DOC soubory. Ty jsou maskovány jako technické dokumentace, lékařské zprávy nebo kontaktní seznamy zaměstnanců. Primárním cílem zavaděče je zamaskovat přítomnost malwaru v systému. K tomuto účelu využívá steganografie.

Steganografie zde slouží k tomu, aby zločinci skryli výměnu dat. V případě MontysThree je hlavní škodlivá komponenta maskována jako bitmapový soubor (formát sloužící k ukládání digitálních obrázků). Pokud je použit správný příkaz, zavaděč použije vlastní algoritmus k dekódování obsahu z pixelového pole a spustí tím škodlivý program.

Hlavní část malwaru používá mnoha šifrovacích technik, aby se vyhnula detekci, konkrétně algoritmus RSA k šifrování komunikace s řídícím serverem a k dešifrování hlavních funkcí malwaru. Mezi ně patří vyhledávání dokumentů se specifickými příponami ve specifických firemních složkách. MontysThree je zaměřen na dokumenty Microsoft a Adobe Acrobat. Může také pořizovat snímky obrazovky a sbírat například informace o síťovém nastavení, názvu počítače a další informace, na jejichž základě ohodnotí zajímavost cíle.

Shromážděné informace a další komunikace s řídicím serverem jsou následně hostovány na veřejných cloudových službách jako jsou Google, Microsoft nebo Dropbox. Žádný antivirový program tyto služby neblokuje, a proto nedochází k detekci

komunikačního provozu. Řídící server může díky tomu nerušeně provádět příkazy [17, 18].

V prosinci 2020 odhalila společnost Kaspersky další malware využívající steganografie. Jedná se o backdoor PowerPepper (zadní vrátka sloužící k nelegitimnímu proniknutí do počítačového systému), který je schopen vzdáleně proniknout do napadeného systému, převzít kontrolu nad zařízeními obětí vybraných firem a díky tomu provádět skrytou špionáž nebo stahování citlivých dat, a za nímž stojí známá kyberzločinecká organizace DeathStalker.

Pro vzdálenou komunikaci s řídícím serverem využívá PowePepper přenos DNS přes protokol HTTPS, aby vše působilo legitimně. K zamaskování své aktivity a k infiltraci používá několik různých technik, mezi něž patří i také steganografie.

K přenosu tohoto malwaru je využíváno spear-phishingových mailů se škodlivými přílohami nebo škodlivými odkazy. K šíření organizace DeathStalker zneužila různých mezinárodních událostí jako například úpravy předpisů o emisích uhlíku, a dokonce i koronavirovou pandemii, aby zmátla své oběti a příměla je tak k otevření těchto dokumentů.

Hlavní část malwaru je zamaskována využitím steganografie. Škodlivý kód je ukryt v běžných obrázcích kapradin nebo paprik a poté je extrahován skriptem zavaděče. Jakmile k tomu dojde, PowePepper začne plnit příkazy posílané operátory skupiny DeathStalker z vzdáleného řídícího serveru. Cílem těchto útoků je ukrást citlivé obchodní informace. Malware může provádět jakýkoli shellový příkaz v napadeném systému, včetně příkazů pro standardní průzkum dat. Příkazy jsou získávány z řídícího serveru prostřednictvím komunikace DNS přes HTTPS.

Právě díky všem těmto technikám nemusí antivirový program nutně malware rozpoznat [19].

Útoků využívajících steganografie existuje neskutečně velké množství a počet neustále přibývá. Mnou popsané příklady jsou jen malou ukázkou toho, co je denní rutinou pro bezpečnostní experty.

2.4 Možnosti využití při ochraně autorských děl

S rozvojem techniky se rozmohlo sdílení souborů přes síť. Šíření digitálních souborů internetem je velice snadné a to sebou nese hrozbu porušování autorských práv. Je proto nutné autorská díla chránit. Pro tyto účely se využívá techniky vodoznaku použitím steganografických metod a metod vodoznaku. Stejně jako u steganografie, tak i u vodoznaku je hlavním cílem ukrytí informace. Pokud se jedná o neviditelný vodoznak, jde podle některých zdrojů o steganografii [3]. Právě tomuto typu vodoznaku se budu v následujícím textu věnovat.

Vodoznaky dělíme na viditelné a neviditelné.

Viditelné vodoznaky jsou navrženy tak, aby byly snadno zpozorovatelné a aby jasně identifikovaly autora.

Neviditelné vodoznaky jsou za běžných podmínek nepostřehnutelné. Dále se dělí na křehké a robustní a na otisky (v originále „fingerprints“).

Křehké vodoznaky jsou navrženy tak, aby byly při sebemenší změně porušeny. Díky tomuto způsobu může dojít k prokázání neoprávněné manipulace s daným souborem. Slouží tedy k autentizaci souboru.

Naopak u robustních vodoznaků je vyžadováno, aby nebyly porušeny při žádných úpravách (například při kompresi, oříznutí či změné velikosti) [20].

Rozšíření vodoznaku představují otisky. V případě pořízení díla chráněného autorským právem je každá kopie opatřena unikátním otiskem, který jasně identifikuje kupujícího. V případě, že by se kupující rozhodl vytvořit nelegální kopie a sdílet je, bude díky otisku zřejmé, kdo je rozšířil [20].

2.4.1 Ochrana autorských a majetkových práv

Vodoznaky chrání autorská a majetková práva, slouží k ochraně digitálních médií proti neautorizovanému užití a distribuci, používají se pro autentizaci obsahu a detekci neoprávněné manipulace. Smyslem je ukrytí proprietárních dat do digitálních médií jako jsou fotografie, digitální obrázky, hudba či videa takovým způsobem, aby například v případě pořízení nelegálních kopií bylo jasné, kdo je skutečným autorem nebo kdo má majetková práva. Existence těchto dat by měla být skryta [3]. Může jít například o vložení loga vydavatele nebo o rozmístění skupiny bitů (znázorňující proprietární data) do obrázku podle daného algoritmu. Vodoznak je do digitálního média skryt tak, aby kvalita původního média nebyla nijak poškozena a aby jej nešlo zachytit zrakem (v případě obrázků) nebo sluchem (v případě audio souborů). Velmi důležitou vlastností vodoznaku je robustnost. Extrakci vodoznaku z originálního souboru umožňuje pouze znalost tajného klíče [20].

Jak již bylo zmíněno, digitální vodoznak má široké využití. Některé způsoby využití jsou podrobněji popsány v následujících částech.

Identifikace a prokázání autorství/vlastnictví

Vodoznaky jsou používány k identifikaci a prokázání autora či majitele. Díky nim je možné prokázat porušení autorských práv [20]. Poskytovatelé obsahu jako jsou jednotliví umělci nebo rozsáhlé broadcastové společnosti mají zájem na prosazení ochrany autorských a majetkových práv u digitálních médií. Chtějí zajistit, aby jejich produkty nebyly komerčně využívány, aniž by byly zaplaceny licenční poplatky. Ke kontrole slouží právě vodoznaky [21].

Trasování nelegálních kopií

K trasování nelegálních kopií se využívá rozšířené techniky vodoznaku neboli otisků. Pro každou distribuovanou kopii je vygenerován unikátní vodoznak, který označí příjemce této kopie. V případě jejího nelegálního šíření bude tedy snadné identifikovat viníka [20].

Monitorování broadcastového vysílání

Vodoznaku se užívá i při broadcastovém vysílání ke monitorování digitálního obsahu. Například inzerenti pomocí něho mohou kontrolovat, jestli se jejich TV spotům dostává vyhrazeného prostoru, který si zaplatili. Chtějí mít jistotu, že je jejich produkt vysílán v celém trvání, v nejoptimálnější denní dobu a na preferovaných strategických frekvencích. Hudebníci a herci si chtějí být jisti, že dostanou přesně zaplaceno za plošné vysílání jejich představení. Vlastníci autorských a majetkových práv by rádi zajistili, aby jejich díla nebyla nelegálně vysílána porátskými stanicemi. Toho je dosaženo vložením unikátního vodoznaku do videa či zvukového klipu před zahájením vysílání. Automatizované monitorovací stanice poté můžou přijímat broadcastové vysílání a dívat se po těchto vodoznacích, identifikovat kdy a kde se každý klip či video objeví [20, 21].

Autentizace

Jako důkazy u soudu mohou být požadovány fotografie či videa z bezpečnostních kamer. Autentičnost (též autenticita) těchto souborů může mít důležitý význam pro soudní jednání. Je tedy nutné, aby s důkazy nebylo nijak manipulováno. K tomuto účelu se využívá křehkého neviditelného vodoznaku. Pokud dojde k jakékoliv manipulaci, projeví se to na vodoznaku, díky čemuž je následně ověřena autentičnost snímku či videa. Takové důkazy mohou u fotografií požadovat také například zpravodajské služby, aby měly jistotu, že snímky nebyly nijak upravovány [20, 22].

3 Moderní steganografické techniky

V této kapitole se věnuji nejpoužívanějším digitálním steganografickým technikám. Na začátku jsou v podkapitole 5.2 uvedeny a popsány vlastnosti metod, podle kterých se následně hodnotí zabezpečení skrývané informace. Podkapitola 3.2 uvádí základní informace o obrazové steganografii a zároveň popisuje několik jejich metod. V podkapitolách 3.3 a 3.4 předkládám základní informace o zbývajících dvou zde popisovaných typech steganografie, zvukové a textové a následně také o jejich příslušných metodách.

3.1 Vlastnosti metod

Pro vkládání dat je vhodné znát základní vlastnosti, které jsou od steganografických metod požadovány, aby se předešlo zbytečnému prozrazení. Pokud by například vložená data významně zvýšila velikost krycího souboru a útočník byl seznámen s vlastnostmi originálního nosiče, steganografie by selhala a útočník by tajnou informaci získal. Navíc je nutné tyto vlastnosti znát pro ohodnocení metod. Při výběru metody je důležité zvolit si jaké vlastnosti jsou nejdůležitější a podle toho si danou metodu vybrat. Každá z metod má totiž odlišné kvality těchto vlastností. Tyto vlastnosti jsou uvedené níže.

3.1.1 Kapacita

Velmi důležitým kritériem je kapacita. Vložením dat by neměla být ovlivněna původní kvalita. Udává, jaké množství dat je možné maximálně ukrýt do vybraného nosiče. Steganografie oproti vodoznaku, kde je nutné vložit jen malé množství dat, cílí na co největší kapacitu [7, 23]. Každá metoda má jinou kapacitu. Například největší kapacity dosahujeme užitím metody LSB (nejméně významný bit – Least Significant Bit), která bude popsána později. Kapacitu ale neovlivňuje pouze vybraná metoda, ale i výběr krycího média.

3.1.2 Nepostřehnutelnost

Tato vlastnost se u steganografie považuje za nejdůležitější. Stojí na ní vše. Data by měla být v nosiči schována takovým způsobem, aby je nebylo možné detekovat. Pokud lidské smysly nebo stroj zachytí přítomnost tajné zprávy, steganografie selhala [7].

Například u zvukové steganografie je důležitá neslyšitelnost změn, jinak by mohlo dojít k prozrazení. Cílem je to, aby lidský sluch nebyl schopen rozeznat rozdíl

mezi originálním zvukových souborem a stego souborem. Tento koncept je založen na vlastnostech lidského sluchu, které jsou měřeny či hodnoceny skrze rodinu standardů PESQ (Perceptual evaluation of speech quality) [6].

3.1.3 Robustnost (odolnost)

Robustnost je schopnost vybraného steganografického algoritmu získat zpátky vložená data v původní podobě, dokonce i po procesu komprese a dekomprese [7]. Jde tedy o odolnost vůči jakékoli manipulaci.

Během přeposílání stego souboru může být tímto souborem nějak útočníkem manipulováno. U obrázku jde například o ořezání nebo rotaci, k čemuž může dojít ještě před tím, než dosáhne cílové destinace. Takovéto úpravy můžou tajnou zprávu zničit. U zvukové steganografie se může jednat o [6]

- přidání šumu do zvuku,
- převzorkování (re-sampling),
- rekvantování (re-quantization),
- střih zvuku.

Pokud dojde například u zvukové steganografie ke konverzi souboru wave na MP3 soubor, můžou být tajná data zničena.

Je proto velmi důležité, aby steganografické algoritmy byly odolné vůči různým, ať úmyslným či neúmyslným manipulacím [6].

[23].

3.1.4 Odolnost vůči statistickým útokům

Statistické útoky se využívají ve stegoanalýze k detekování různých abnormalit či „stop“, které vznikají po steganografických úpravách během vkládání dat. Steganografické metody by proto takové stopy neměly za sebou zanechávat, aby se vyhnuly detekci útočníkem [23].

3.1.5 Nezávislost na formátu souboru

Velmi důležitá je i schopnost metody ukrývat tajná data do odlišných formátů souborů. Pokud jsou mezi dvěma komunikujícími stranami neustále posílány stejné typy formátů, může to působit podezřele. Nejsilnější steganografické metody jsou proto schopné vkládat data do jakéhokoliv typu souboru [23].

3.1.6 Nenápadnost souborů

Ukrytí informací do typů souborů, které jsou používány velmi zřídka, může vzbudit podezření. To samé může nastat i v případě různých odchylek od normálu, například abnormální velikost souboru, který bývá obvykle menší. Proto je důležité pro menší nápadnost používat spíše často používané typy souborů a zároveň dbát na velikost výsledného stego souboru [23].

3.1.7 Časová náročnost

V určitých případech může být důležitá i doba, za kterou daná metoda skryje či odkryje tajná data [24]. Tuto dobu můžeme popsat jako počet vložených bitů tajné zprávy do krycího média za jednu sekundu. Samozřejmě velmi záleží i na výběru programovacího jazyka, protože každý jazyk je jinak rychlý.

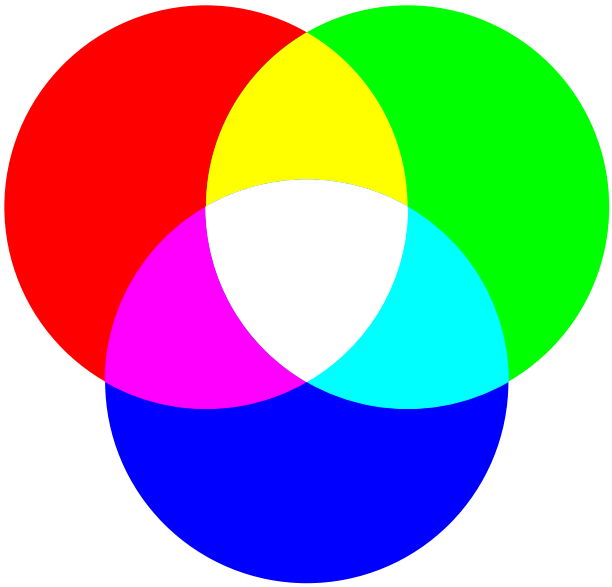
3.2 Obrazová steganografie

Obrazová steganografie stála na počátku vývoje digitálních typů steganografie. Jedná se o nejprozkoumanější a nejrozšířenější typ steganografie. Je to z toho důvodu, že komunikace obrázky je velmi rozšířená. Tato forma komunikace se používá například v známé aplikaci využíváné pro publikování obrázku Instagram a samozřejmě v mnoha dalších aplikacích.

Obrazová steganografie využívá pro ukrytí tajné zprávy do obrázku nedokonalosti lidského zraku. Lidské oko jemné změny v hodnotách pixelů nepostřehne, a proto mohou podobné modifikace obrázku projít bez povšimnutí. Podobných vlastností lidského vnímání využívají i další druhy digitální steganografie [12].

Na začátku je vhodné vysvětlit, jak chápat pojem digitální obrázek. Rozlišujeme dva typy, vektorové a rastrové. V této práci budou popisovány rastrové obrázky, protože jsou běžnější než vektorové a ve steganografii se více využívají. Rastrový obrázek je tvořen mřížkou pixelů, která je běžně označována jako bitmapa. Tyto pixely mají různou formu, která je dána typem obrázku. Hodnoty pixelů černobílých obrázků nabývají hodnot 0 nebo 1, u šedotónových nabývají hodnot v intervalu <0,255> a například u barevného RGB obrázku viz obrázek 3.1, který se skládá ze tří složek R (pro červenou), G (pro zelenou), B (pro modrou barvu), bude pixel složen z hodnot těchto tří složek, opět v intervalu <0,255>. Na obrázku 3.2 můžeme vidět barevný a šedotónový obrázek.

Barevný rozsah určuje bitová neboli barevná hloubka. To znamená, kolik odstínů má daná barva. Určuje, kolik bitů je potřeba k popisu konkrétní barvy v obrázku, takže se jedná o počet bitů na pixel. U černobílého obrázku je to jeden bit, což jsou



Obr. 3.1: RGB model.

Obr. 3.2: Barevný a šedotónový obrázek.

dvě barvy, černá a bílá. U šedotónových obrázku je bitová hloubka 8 bitů, což dává dohromady 256 barev (odstínů šedi). U většiny barevných obrázků je bitová hloubka 24 bitů (každá ze složek RGB modelu se skládá z 8 bitů), což se označuje jako „True Color“. Tato hloubka pokryje 16 777 216 barevných odstínů [24, 25].

Bylo vyvinuto velké množství metod, které byly navrženy jak pro obrázky procházející bezeztrátovou kompresí, tak i kompresí ztrátovou. Zde můžeme zmínit na příklad formáty JPEG, PNG nebo BMP, což jsou nejběžnější obrazové formáty. Obrázek je pro výpočetní techniku řada čísel, která reprezentuje intenzitu světla nebo samotné pixely. Pro užití steganografických metod jsou typické obrázky používající 8bitovou či 24bitovou barevnou hloubku. Oba druhy mají své výhody i nevýhody. Výhodou 8bitových obrázků je jejich malá velikost, nevýhodou je, že je použito jen 256 barev. Obvykle je ale používána paleta šedých odstínů. Změnu barvy zde bude po vložení tajné zprávy těžší detekovat. U 24bitových obrázku můžeme mluvit o dostatečně velkém prostoru pro ukrytí zprávy a také o dostatečné flexibilitě pro ukrytí zprávy. Nevýhodou je ale větší velikost. V takovém případě může být řešením ztrátová komprese obrázku [12, 22].

Navržené metody pro vkládání informací do obrázku mohou být seskupeny podle typů úprav, ke kterým při jejich použití dochází.

Úpravy mohou být založeny na změně hodnot pixelů, čímž ovlivňují prostorovou doménu (Spacial Domain) obrázku. Dalším složitějším způsobem ukrytí dat do obrázku jsou transformace (Transform Domain), které ukrývají data užitím a modifikací algoritmů používaných při kompresi obrázku. Mezi tyto algoritmy můžeme zařadit například diskrétní kosinovou transformaci (DCT), která může vyústit ve změnu jasu či jiných měřitelných vlastností obrázků. Další možností je oba tyto typy úprav zkombinovat [12].

Metod obrazové steganografie je opravdu velké množství a já si pro vysvětlení vybrala následující tři metody.

3.2.1 Metoda LSB (Least Significant Bit)

Metoda LSB neboli česky metoda nejméně významného bitu nahrazuje deterministicky nejméně významné bity obrázku bity tajných dat. Protože se jedná o nejméně významné bity, rozdíl je minimální a lidské oko tuto změnu nepostřehne. Pro tuto metodu jsou spíše vhodné bezeztrátové formáty obrázků. U ztrátových formátů obrázků by došlo po kompresi k poškození tajné zprávy [2]. Princip této metody je ukázán na obrázku 3.3.

Tuto metodu je možné implementovat různými způsoby. Pro co největší nepostřehnutelnost je vhodné například u 24bitového obrázku vložit tři bity do každého pixelu (do každé složky jeden). Každý pixel je zde reprezentován třemi bajty. Na

Vložení písmena A

Znak A - binárně 01000001

Mějme tři pixely:

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

Nahrazované bity jsou tučně vyznačeny.

Po výměně původních nejméně významných bitů za bity znaku A získáme tento výsledek:

(00100110 11101001 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)

Obr. 3.3: Ukázka principu fungování metody LSB pro vložení znaku A nahrazením nejméně významných bitů bajtů pixelů 24bitového obrázku za bity znaku A.

obrázku 3.4 lze vidět barvy lišící se jen v nejméně významných bitech. Rozdíl je nepostřehnutelný.

Pro zjištění kapacity při tomto postupu musíme spočítat počet pixelů obrázku a následně tento součin vynásobit třemi (měníme totiž právě 3 bity). U 24bitového obrázku o velikosti 800×600 pixelů bychom mohli vložit 1 440 000 bitů nebo 180 000 bajtů, což je přibližně 175 kilobajtů [25].

Obr. 3.4: Porovnání dvou barev při změně nejméně významných bitů. RGB hodnoty levého obrázku jsou (253, 183, 206) a pravého (252, 182, 205).

V případě, že bychom potřebovali větší kapacitu, mohli bychom nahradit více bitů každé složky. Při změně dvou posledních bitů každé složky by změna ještě postřehnutelná nebyla, ale s každým dalším změněným bitem se zvyšuje dopad změn viz obrázek 3.5.

N-tý bit	Procentuální vliv
7	50%
6	25%
5	12.5%
4	6.25%
3	3.125%
2	1.5625%
1	0.7813%
0	0.3906%

Obr. 3.5: Vliv bitů na 8 bitovou hodnotu [24].

Další možností je rozložení bitů na jednotlivé barevné složky, bity můžeme přepisovat postupně po barvách [24].

3.2.2 Metoda PVD (Pixel Value Differencing)

Metoda PVD byla navržena pro obrázky v šedých odstínech. Vložená data můžou být extrahována ze stego obrázku i bez znalosti původního souboru. Tato metoda cílí na větší nepostřehnutelnost oproti základní metodě LSB.

Změny v určitých částech obrázku mohou být více nápadné než v jiných. Jde o homogenní plochy jako je například voda nebo obloha. Tato metoda se snaží s tímto faktem vypořádat tím, že vypočítá rozdíl hodnot dvou sousedících pixelů. Tyto rozdíly poté ohodnotí na základě kvantizační tabulky a podle té se rozhodne, zda se jedná o homogenní či heterogenní oblast. Pokud je rozdíl velký, jedná se o různorodou část. V této části člověk hůře rozezná rozdíly, a proto je možné v takovém případě na místo uložit větší množství dat. Tato data jsou následně vložena do obrázku jako nové hodnoty zvolených pixelů [26].

3.2.3 Metoda JSTEG

Metoda JSTEG je jednou z metod pro formát obrázku JPEG. Princip je podobný principu LSB metody. JPEG formát je ztrátový a při kompresi může být tajná zpráva poškozena. Proto se tajná data u této metody vkládají do obrázku ve chvíli, kdy už při kompresi došlo k diskrétní kosinové transformaci a kvantizaci. Tyto fáze jsou

totiž ztrátové. Poté může dojít k další fázi komprese, při které se používá Huffmanova kódování. Tato fáze už je bezeztrátová [22].

3.3 Zvuková steganografie

Vedle vývoje obrazové steganografie se začala vyvíjet i zvuková steganografie. V současné době se nemusíme bát, že by přenos zvukového souboru mezi dvěma stranami vyvolal nějaké podezření, a proto se tento typ steganografie mohl směle rozvíjet dál.

Lidské ucho není totiž stejně jako lidské oko dokonalé, a proto není v některých případech schopno zaznamenat rozdíl mezi originálním souborem a stego-souborem. Na rozdíl ale od oka je přece jen na tyto rozdíly náchylnější. Je například velmi citlivé na šum. Proto zde není tolik možností využití těchto nedokonalostí jako u zrakového systému, nicméně stále existuje několik možností vkládání tajných dat do zvuků, při kterých lidské ucho selže a nezaznamená nějakou změnu.

Časem vzniklo velké množství metod určených pro zvukovou steganografii. Některé z nich se dají využít i pro jiné typy steganografie. Jde například o metodu LSB (kódování nejméně významného bitu), která byla původně vytvořena pro účely obrazové steganografie.

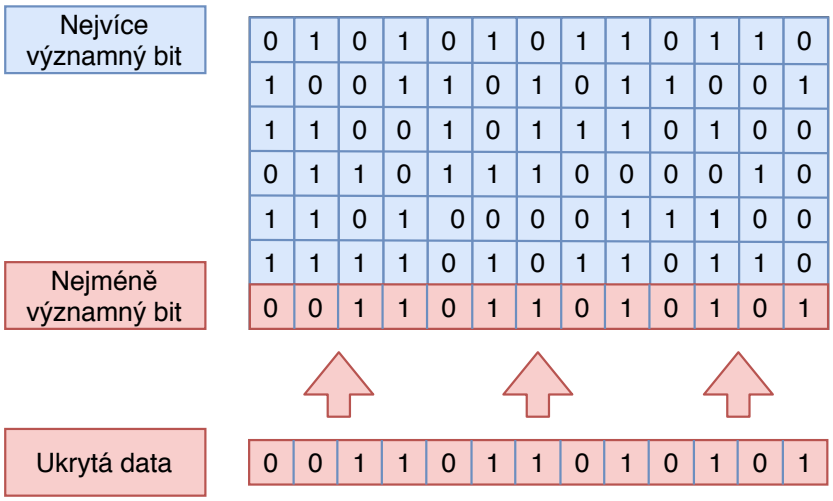
Vybrané metody jsou popsány níže. Další metody zvukové steganografie jsou například zmíněny v práci [6].

3.3.1 Kódování nejméně významného bitu (Least significant bit method)

Tato metoda je založena na vložení každého bitu tajné zprávy deterministicky do nejméně významného bitu krycího média viz obrázek 3.6. Proto je u vzorkovací frekvence 16 kHz je v krycím souboru uschováno 16 kbps tajných dat. V některých případech je možné použít i dva nebo více bitů, čímž zajistíme větší kapacitu, ale rozdíl mezi původním souborem a stego souborem už bude slyšitelný. Tato metoda umožňuje vložení velkého množství dat, tudíž můžeme mluvit o dostatečně velké kapacitě a je relativně jednoduchá, co se týče implementace. Nicméně, tato metoda je bohužel charakteristická nízkou odolností vůči hluku, což snižuje její bezpečnost. Pokud by došlo k přidání hluku, amplifikaci, filtrování či ztrátové kompresi u stego souboru, dojde s velkou pravděpodobností ke zničení dat [6].

3.3.2 Kódování paritního bitu (Parity coding)

Při této metodě je zvukové krycí médium rozděleno na několik stejně dlouhých částí. Tajná zpráva je bit po bitu ukryta do paritních bitů každého z těchto úseků. Pokud



Obr. 3.6: Proces vkládání tajné informace do nejméně významného bitu souboru se vzorkem o délce 7b.

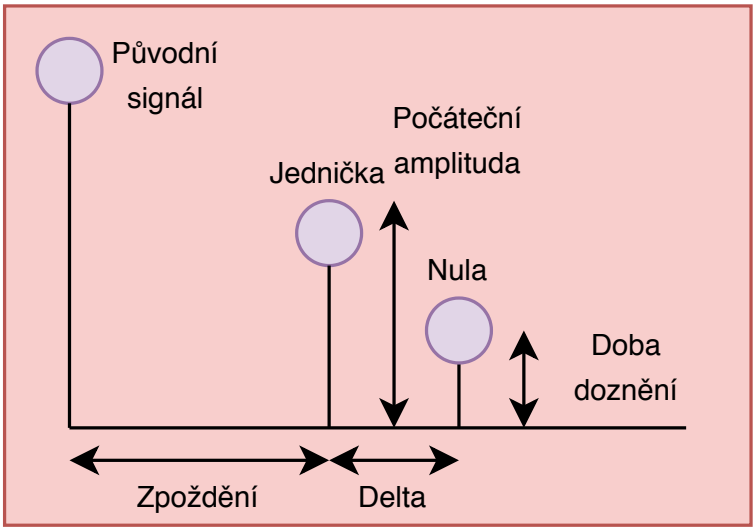
je paritní bit daného úseku shodný s vkládáným bitem zprávy, nic se nemění. Pokud je ale paritní bit od vkládaného odlišný, je potřeba nejlépe nejméně významný bit toho úseku invertovat [27].

Tato metoda se podobná předcházející metodě a to v tom, že využívá kódování nejméně významného bitu vzorku. Výhodou také je větší bezpečnost, protože máme mnoho možností, jak úseky původního zvuku rozdělit. Útočník nemá šanci přijít na skrytá data, pokud nemá informace o tom, na jaké úseky byl zvuk rozdělen. Pro rozkódování zprávy je proto potřeba vědět, na jak dlouhé úseky byl zvukový soubor rozdělen.

3.3.3 Ukrývání ozvěny (Echo hiding)

Metoda ukrývání ozvěny vkládá tajná data do zvukového média vytvořením krátké umělé ozvěny. Jde o rezonanci přidanou k původnímu zvuku. Tímto je proto vyřešen problém citlivosti lidského sluchu na aditivní šum. Poté, co je ozvěna přidána, stego signál si zachovává stejné statistické i vjemové vlastnosti. Díky tomu je zde velká robustnost.

Pro efektivní ukrytí zprávy jsou brány v potaz a změněny následující tři parametry, které s ozvěnou souvisejí, a to počáteční amplituda, zpoždění a doba do znění původního zvuku viz obrázek 3.7. Všechny tyto faktory by měly být nastaveny pod hranici slyšitelnosti lidského sluchu, aby byla ozvěna nepostřehnutelná. Zpoždění do 1 ms mezi originálním signálem a přidanou ozvěnou je nerozeznatelné. Hodnoty zpoždění jsou navíc měněny tak, aby korespondovaly s bity tajné zprávy. Specifická hodnota zpoždění představuje binární jedničku, jiná hodnota zase repre-



Obr. 3.7: Parametry související s ozvěnou.

zentuje binární nulu. Nevýhodou této metody ale je nízká kapacita a zabezpečení [6, 27].

3.3.4 Ukrývání v úsecích ticha (Hiding in silence intervals)

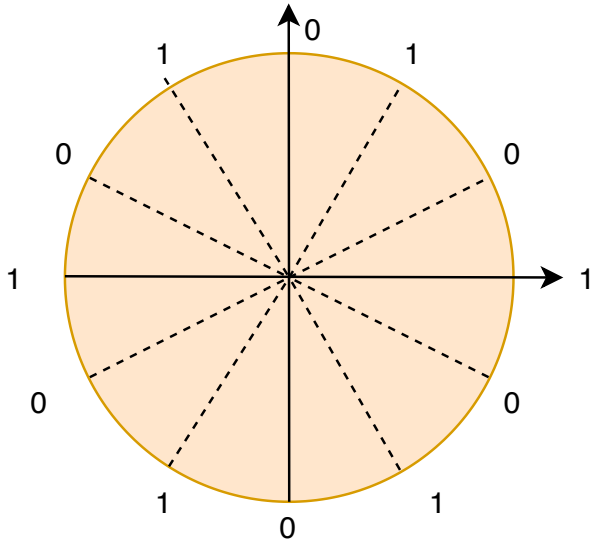
Metoda ukrývání v úsecích ticha využívá intervaly ticha zvukového souboru. Je vhodná pro nahrávky mluveného projevu. Na začátku jsou určeny intervaly ticha řeči a jejich příslušné délky (počet vzorků v intervalu ticha). Ty jsou následně využity pro vložení bitů tajných dat. Krátké intervaly ticha jsou ale ponechány beze změn, protože jde často krátké pauzy během řeči a jakékoliv změny by ovlivnily plynulost a kvalitu projevu. Nevýhodou je citlivost vůči kompresi. Změny v intervalech ticha můžou vést k extrakci přidaných dat. Tento problém ale může být vyřešen zesílením vzorků řeči a redukcí vzorků intervalů ticha. [6].

3.3.5 Metoda přidání tónu (Tone insertion)

Tato technika je založena na vlastnostech lidského sluchu, díky kterým v přítomnosti výrazně vyššího tónu neslyšíme tón nižší. Ten je do zvukového média vložen za účelem skrytí tajných dat. Vložením těchto tónů na známé frekvence je dosaženo tajného vložení a správné extrakce dat. Metoda přidání tónu je schopna odolat útokům jako jsou například filtrování dolní propusti (low-pass filtering) nebo krácení bitů (bit truncation). Nevýhodou ale je nízká kapacita. Vložená data navíc mohou být útočníkem snadno odhalena, protože vložené tóny jsou lehce detekované. Tato nevýhoda může být odstraněna změnou čtyř nebo více frekvencí ve specifickém pořadí [6].

3.3.6 Metoda kódování fáze (Phase coding)

Tato metoda je založena na faktu, že na rozdíl od šumu, lidské ucho nepostřehne fázi zvuku. Spíše než přidání šumu, tato technika pozmění fáze vybraných frekvencí zvukového signálu podle určených hodnot, které znázorňují bity tajné zprávy, čímž se dosáhne z hlediska poměru signálu k šumu neslyšitelnosti. Tyto hodnoty jsou znázorněny na obrázku 3.8. Jedná se o jednu z nejúčinnějších metod, co se týče to-



Obr. 3.8: Hodnoty pro změnu fáze.

hoto poměru. Modifikace fází by měly být ale dostatečně malé, aby se neslyšitelnosti opravdu dosáhlo, jinak by mohlo dojít k disperzi zvuku. Mezi výhody určitě patří i vysoká odolnost vůči změnám signálu [6, 27].

3.3.7 Metoda rozprostřeného spektra (Spread spectrum)

Rozprostřené spektrum je koncept vyvinutý pro datovou komunikaci k zajištění řádného obnovení zasílaného signálu přes hlučný kanál vytvořením redundantních kopií datového signálu. Data jsou v podstatě násobena „M-sequence“ kódem, který je znám jak odesílateli, tak i příjemci. Poté jsou tato data ukryta do zvukového nosiče. Pokud jsou tedy některé hodnoty šumem poškozeny, budou existovat další kopie sloužící k obnovení tajné zprávy [6].

Metoda rozprostřeného spektra rozprostírá bity tajné zprávy skrze frekvenční spektrum zvukového média. Postup této metody je ekvivalentní k metodě nejméně významného bitu tím, že bity tajné zprávy také ukrývá přes celý zvukový signál. Na rozdíl od ní ale rozprostírá bity tajné zprávy po frekvenčním spektru zvukového signálu pomocí kódu, který není na původním signálu závislý. V důsledku toho bude

výsledný signál využívat větší šířku pásma, než je pro komunikaci nezbytně nutné [27].

3.4 Textová steganografie

Souběžně s obrazovou a zvukovou steganografií se vyvíjela textová steganografie. Dostupné metody různými způsoby zneužívaly vlastnosti textových souborů. První metody využívaly mezer mezi slovy pro zakódování informací, čehož bylo údajně využito i za časů Margaret Tchatcherové k vysledování pachatelů odpovědných za úniky citlivých dokumentů z britského Kabinetu.

Pokročilejší steganografické metody využívaly syntaktické a sémantické struktury textu jako nosiče. Jednalo se například o přesun interpunkčních znamének, změnu slovosledu nebo použití synonym, kterým byly poté přiřazeny hodnoty, buďto binární jednička nebo nula [12].

Textová steganografie může měnit formát existujícího textového souboru nebo třeba generovat náhodnou posloupnost znaků. Jako nosič zde používáme textový soubor. Vložení tajných dat do textového souboru takovým způsobem, aby se na jejich přítomnost nepřišlo, může být velice složité. Textové soubory všeobecně na rozdíl od obrazových či zvukových souborů disponují malým množstvím redundantních dat, která by mohla být nahrazena tajnou informací. Vzor zakódování tajných dat může být v některých případech snadno odhalen. Jakékoliv změny v textu mohou původní text poškodit, a nebo můžou působit příliš nápadně. Další nevýhodou je lehkost, se kterou lze text změnit pouhým pozměněním samotného textu nebo přeformátováním na jiný formát. Výhodou je ale menší paměťová náročnost [7, 22].

Existuje velké množství metod, které umožňují ukrýt informace do textového souboru. Vybrané jsou popsány níže.

3.4.1 Metody založené na formátování textu (Format Based Methods)

U těchto metod se upravuje formát textu. Můžeme zde zařadit vkládání mezer, úmyslné hrubky či změny velikosti písma. K této skupině metod patří například metody volného prostoru (Open Space Methods).

Metody volného prostoru

Existuje několik možností jak využít pro zakódování informace volný prostor v textu. Běžný čtenář totiž nepostřehne nadbytečnou mezeru na konci řádku nebo větší mezeru mezi dvěma slovy. Tyto metody jsou ale vhodné pouze pro ASCII formát.

- **Metoda mezi-větných mezer (Inter-sentence spacing)** zakóduje binární nulu přidáním jedné mezery po tečce na konci věty. Přidání dvou mezer by reprezentovalo binární jedničku. Nevýhodou této metody je to, že pro vložení malého množství dat tajné zprávy vyžaduje velké množství textu. Navíc existuje mnoho nástrojů pro korekci textu, které nadbytečné mezery mezi větami opravují.
- **Metoda posunu řádku (Line-shifting encoding)** posouvá řádky textu vertikálně nahoru nebo dolů přibližně o 3 milimetry. Hodnota tajných dat (binární jednička nebo nula) je určena podle toho, zda je řádek posunut nahoru nebo dolů.
- **Metoda mezer na konci řádku (End-of-line spacing)** využívá bílých znaků. Data jsou zakódována předem určeným počtem mezer na konci řádku. Například dvě mezery zakódují jeden bit tajné zprávy, čtyři mezery zakódují dva bity a tak dále. Tato technika funguje lépe než metoda mezi-větných mezer, protože zvyšující se počet mezer ukryje větší množství dat.
- Další specifické metody upravují za účelem zakódování dat například některé atributy textu jako jsou velikost či typ písma.

Tyto metody vyžadují znalost původního formátování textu pro dekódování tajné zprávy [22].

3.4.2 Náhodné a statistické generování

Tyto metody jsou založeny na ukrytí tajných dat vygenerováním vlastního cover textu. Vytvářejí náhodnou posloupnost znaků či náhodnou posloupnost slov. Vygenerovaný text se podle určitých statistických údajů snaží působit jako skutečný text.

Slova z náhodně poskládaných znaků se můžou pro některé systémy odhalování skrytého textu jevit jako gramaticky správná z toho důvodu, že pro svůj vznik používají zjištěných statistických hodnot jako je například četnost výskytu znaků či průměrná délka slov. U posloupnosti náhodných slov je využito skutečných slov ze slovníku. I tak je ale velká pravděpodobnost odhalení, protože takto vygenerovaný text sice používá skutečná slova, ale jeho sémantická struktura smysl nedává [7].

3.4.3 Lingvistická steganografie

Výpočetní technika je stále více pokročilejší a je schopna analyzovat složité jazykové struktury. Lingvistická steganografie bere v úvahu lingvistické vlastnosti generovaných a upravovaných textů a v mnoha případech používá jazykové struktury jako prostor vhodný pro ukrytí zprávy. Mezi tento druh steganografie řadíme následující metody.

Syntaktické metody

Syntaktické metody využívají interpunkčních znamének a struktury textu pro skrytí dat. Binární nula nebo jednička jsou reprezentovány například slovními spojeními, které jsou téměř identické až na umístění čárky (obě spojení jsou gramaticky správná). První spojení bude reprezentovat binární jedničku, druhé spojení s odlišným umístěním čárky binární nulu. [28].

Sémantické metody

Sémantické metody přiřazují dvěma navzájem odpovídajícím synonymům primární a sekundární hodnotu. Tyto hodnoty jsou poté přeloženy jako binární jednička a nula. Například slovo „velký“ bude označeno jako primární a slovo „obrovský“ jako sekundární. Při dekódování zprávy by potom užití primárního slova znamenalo jedničku a použití sekundárního nulu. Problém tohoto postupu spočívá v tom, že nahrazení jednoho synonyma za druhé může v některých případech narušit logickou strukturu věty, protože ne vždy jsou si synonyma ve všech kontextem rovnocenná [28].

4 Popis aplikace

Kapitola je věnována popisu aplikace využívající mnou vybranou metodu steganografie. Podkapitola 4.1 uvádí požadavky na aplikaci a vybranou metodu pro mou aplikaci. Následující podkapitola 4.2 popisuje programovací jazyk, který jsem si pro implementaci zvolila. Poslední podkapitola 4.3 popisuje možnosti využití aplikace.

4.1 Požadavky na aplikaci a vybraná metoda

Hlavním požadavkem na aplikaci bylo, aby využívala mnou zvolenou metodu steganografie ke skrytí a odhalení informace. Samotná steganografie ale nemusí být vždy nutně schopna zajistit dostatečné zabezpečení skrývané informace, a proto je vhodné tajná data navíc zašifrovat, aby byla zajištěna důvěrnost těchto dat.

K dalšímu zvýšení zabezpečení se často přidává i zajištění autentičnosti a integrity. Autentičnost ověřuje, zda data skutečně pocházejí od daného zdroje. Integrita nám dává jistotu, že s informací nebylo nijak manipulováno a ta zůstává stejná jako na začátku.

Všechna tato bezpečnostní opatření byla dalším požadavkem na mou aplikaci.

Pro skrytí a odhalení informace jsem si zvolila metodu z obrazové steganografie, a to metodu LSB, která nahrazuje nejméně významné bity krycího obrázku bity skrývané zprávy. Princip této metody byl popsán v podkapitole 3.2.1.

4.2 Programovací jazyk

Jako programovací jazyk jsem si vybrala Javu, která patří mezi nejvíce používané programovací jazyky na světě. Jde o objektově orientovaný programovací jazyk, který je nezávislý na architektuře a přenositelný, tudíž pro mou aplikaci ideální. Pro správnou funkčnost stačí, aby měl operační systém k dispozici interpret Javy (virtuální stroj Javy).

Javu jsem si vybrala, protože s ní mám již předešlé zkušenosti. Samotný program jsem vytvářela ve vývojovém prostředí Eclipse IDE.

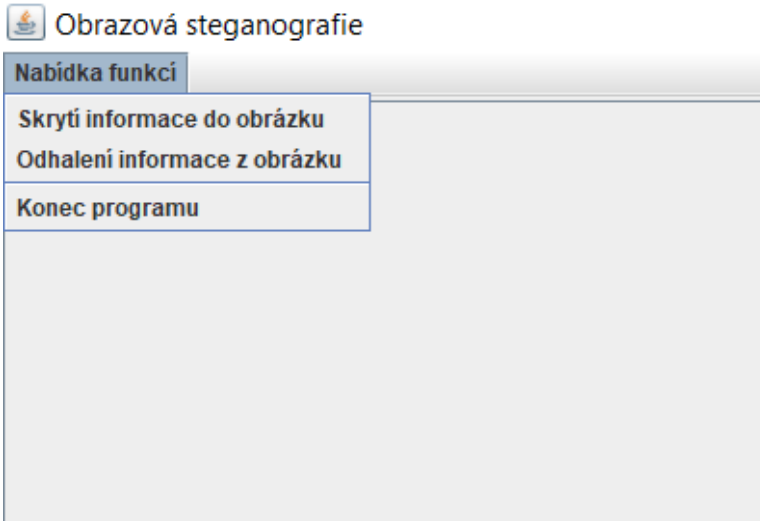
4.3 Uživatelské prostředí

Pro grafické uživatelské rozhraní jsem zvolila knihovnu Swing viz [29]. Komponenty knihovny Swing jsou nezávislé na platformě a na všech platformách fungují stejně. Jedná se o knihovnu uživatelských prvků určené pro ovládání programu pomocí

grafického rozhraní. Umožňuje vytvářet okna, dialogy, rámečky, tlačítka a mnoho dalších komponent.

Aplikace umožňuje skrýt jakýkoli text (i s českou diakritikou) do námi zvoleného obrázku. Podporované formáty pro krycí obrázek jsou PNG, JPG a BMP. Výstupním formátem steganogramu je formát PNG.

Lze si vybrat mezi dvěma režimy (skrytí informace a odhalení informace). Přepíná se mezi nimi přepínačem v horní části okna viz obrázek 4.1.



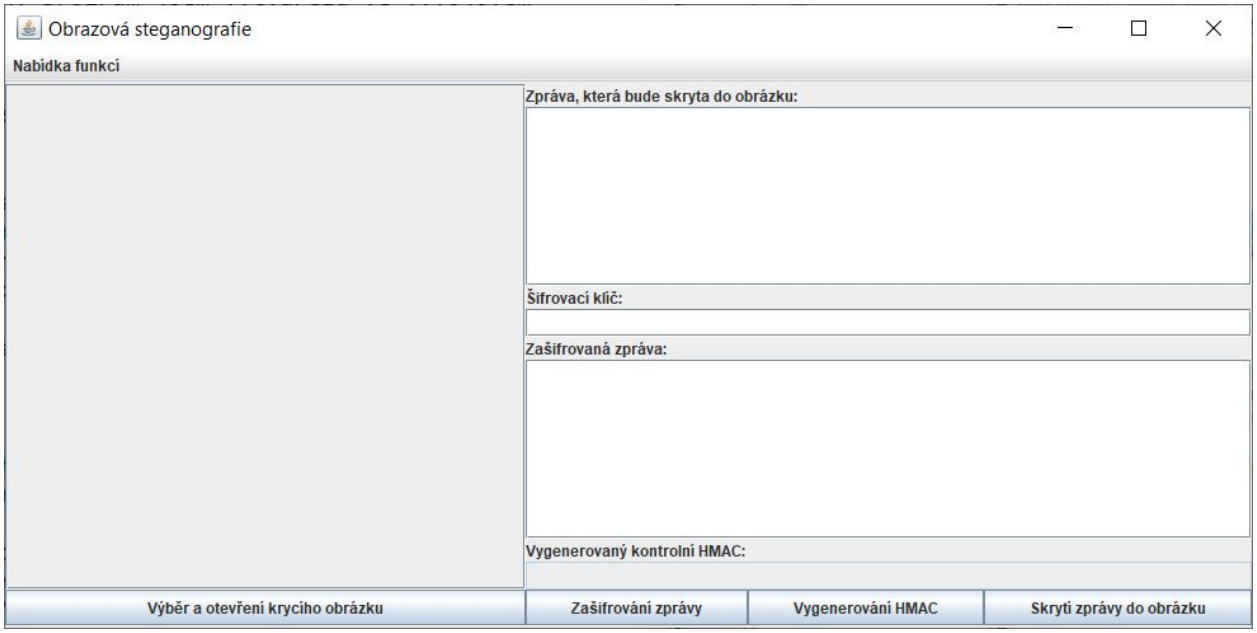
Obr. 4.1: Režimy aplikace.

Režimy jsou následující.

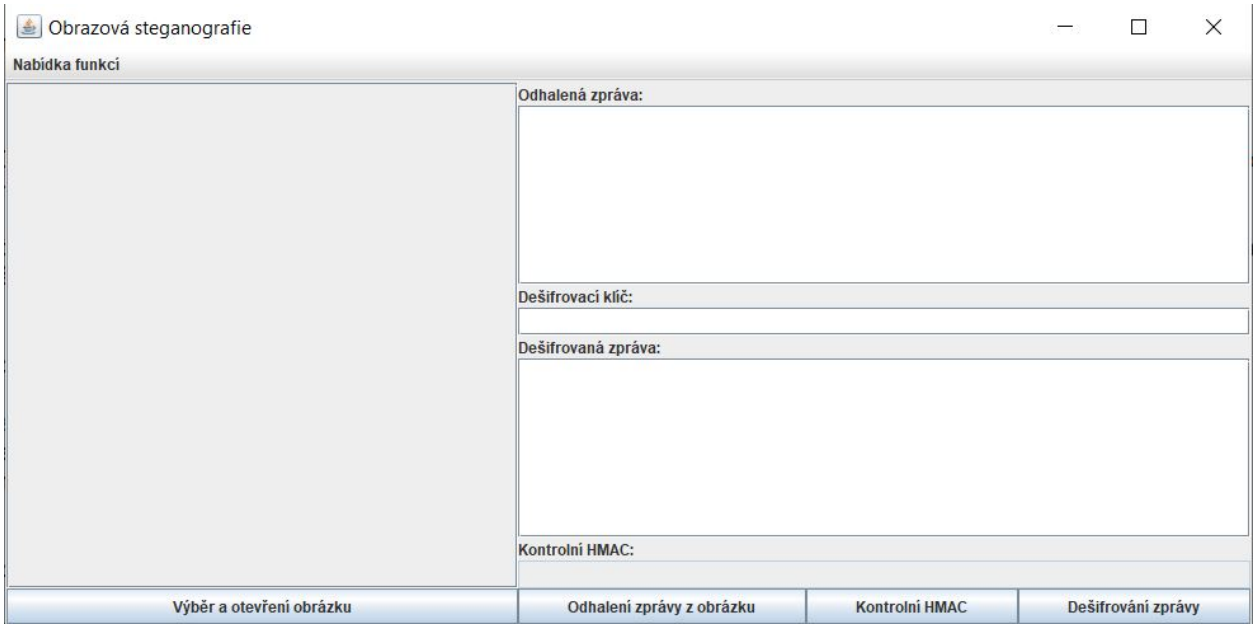
- První režim slouží ke skrytí informace do obrázku 4.2. V něm si uživatel vybere krycí obrázek a vloží text určený k ukrytí. Zde má možnost volitelného zašifrování textu pro zvýšení úrovně zabezpečení utajované informace. Dalším volitelným krokem je vygenerování kódu HMAC ukrývané informace. Poté je provedeno skrytí dat.
- Druhý režim umožňuje odhalení informace z obrázku 4.3. Uživatel v tomto režimu vloží stego obrázek, odhalí skrytá data. Pokud byla data zašifrována, dešifruje je. Opět má možnost vygenerování kódu HMAC a následného porovnání s HMAC původní skrývané informace.

4.3.1 Skrytí informace do obrázku

Režim „Skrytí informace do obrázku“ umožňuje vložení krycího obrázku pomocí tlačítka „Výběr a otevření krycího obrázku“. Po výběru je zvolený obrázek v aplikaci zobrazen.



Obr. 4.2: Režim skrytí informace do obrázku.

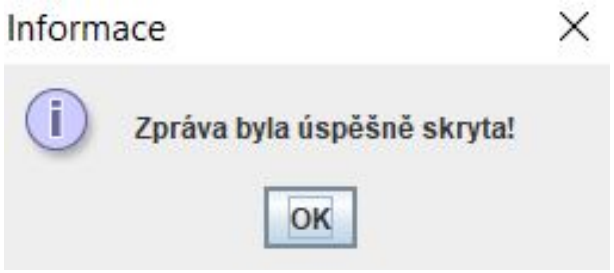


Obr. 4.3: Režim odhalení informace z obrázku.

Požadovaná tajná zpráva se vepíše do pole „Zpráva, která bude skryta do obrázku“. V poli „Šifrovací klíč“ lze volitelně zvolit klíč pro zašifrování zprávy. Po zadání klíče se tlačítkem „Zašifrování zprávy“ námi zadaná zpráva zašifruje.

Dále je možné volitelně vygenerovat HMAC pro ukrývanou informaci. Po stisknutí tlačítka „Vygenerování HMAC“ vyskočí okno s instrukcí „Vložte jméno souboru pro uložení HMAC“. Po vyplnění jména a stisknutí tlačítka „OK“ je následně HMAC v textovém formátu uložen a zároveň zobrazen v poli „Vygenerovaný kontrolní HMAC“. Vygenerovat HMAC lze jak pro zašifrovanou zprávu, tak pro nezašifrovanou.

Celý proces dokončíme tlačítkem „Skrytí zprávy do obrázku“. Zobrazí se nám instrukce „Vložte jméno steganogramu“. Po vložení jména a stisknutí tlačítka „OK“ dostaneme informaci o tom, zda byla zpráva úspěšně skryta viz obrázek 4.4 a výsledný steganogram je uložen.



Obr. 4.4: Informace o skrytí zprávy.

Skrytí informace je znázorněno na obrázku 4.5.

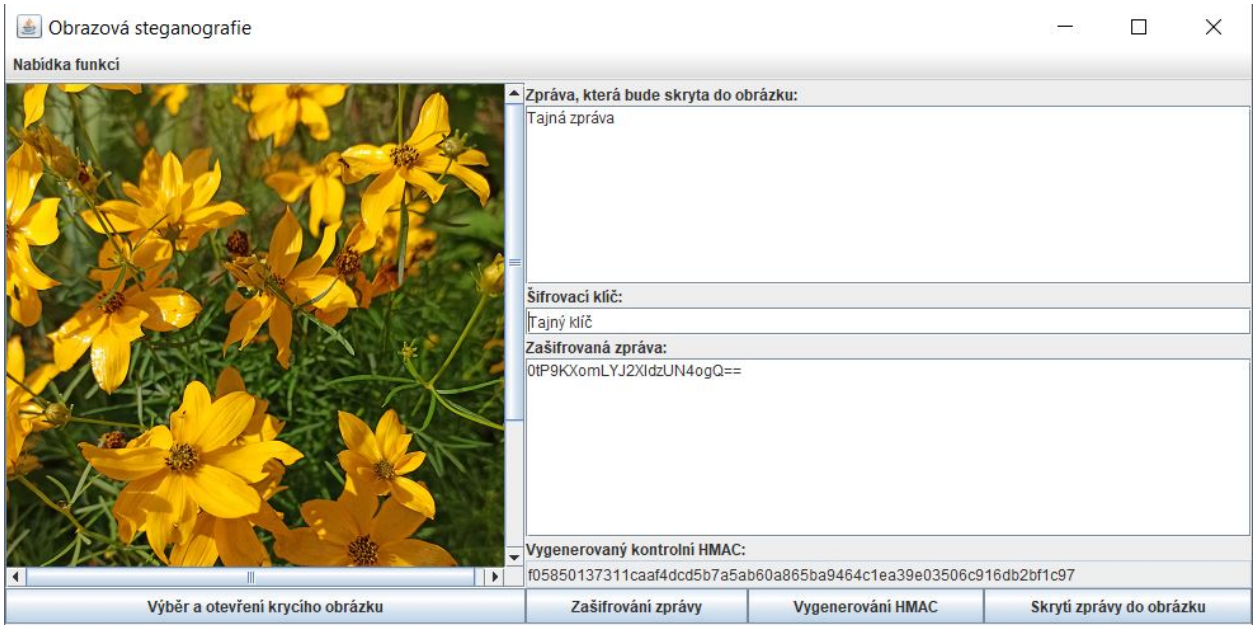
V případě, že není vyplněn šifrovací klíč, ukryje se do obrázku zpráva v otevřené podobě. Pokud je ukrývaná informace větší než počet dostupných bitů v krycím obrázku, zobrazí se nám informace „Zprávu nebylo možné vložit do obrázku“.

Různé situace jako je například absence krycího obrázku a následné stisknutí tlačítka „Skrytí zprávy do obrázku“ či stisknutí tlačítka „Zašifrování zprávy“ bez zadaného šifrovacího klíče jsou ošetřeny.

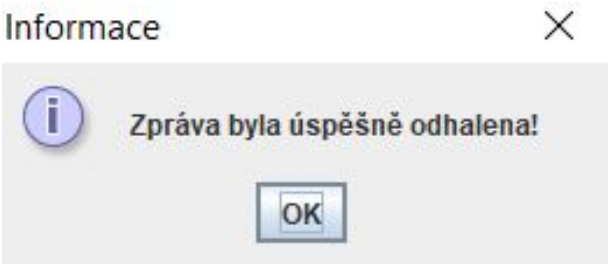
4.3.2 Odhalení informace z obrázku

Režim „Odhalení informace z obrázku“ umožňuje odhalení ukryté informace ze steganogramu. Pomocí tlačítka „Výběr a otevření obrázku“ vybereme námi vybraný steganogram, který je následně v aplikaci zobrazen. Pro odhalení ukryté informace slouží tlačítko „Odhalení zprávy z obrázku“, po jehož stisknutí se nám zobrazí informace o tom, zda byla zpráva úspěšně odhalena či ne viz obrázek 4.6.

Tato zpráva se následně objeví v poli „Odhalená zpráva“. Pokud nebyla zašifrována, objeví se nám rovnou v otevřené podobě. V případě zašifrování je ještě nutné



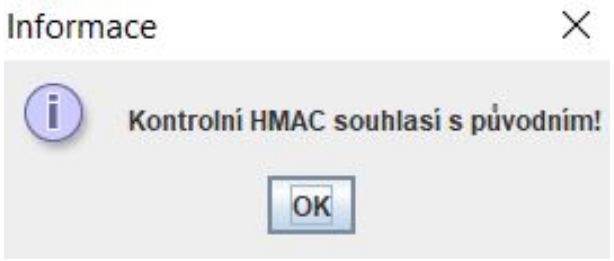
Obr. 4.5: Skrytí informace do obrázku.



Obr. 4.6: Informace o odhalení zprávy.

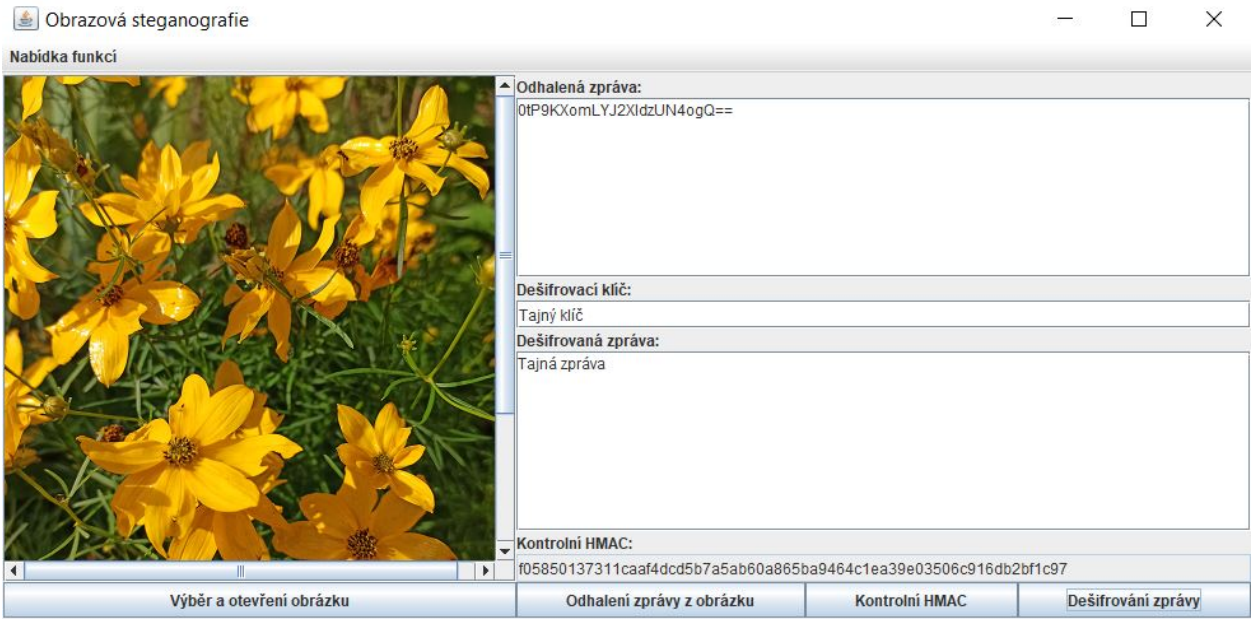
zprávu odšifrovat, a to vyplněním tajného klíče do pole „Dešifrovací klíč“ a použitím tlačítka „Dešifrování zprávy“. Poté se objeví v poli „Dešifrovaná zpráva“.

Další součástí tohoto režimu je kontrola HMAC, která porovná HMAC původní skrývané informace s HMAC nově odhalené informace. Toho docílíme stisknutím tlačítka „Kontrolní HMAC“ a po výběru spočítaného HMAC původní informace se ukáže informace o tom, zda kontrolní HMAC nově odhalené informace souhlasí s původním viz obrázek 4.7. Nově spočítaný HMAC odhalené zprávy se zobrazí v poli „Kontrolní HMAC“.



Obr. 4.7: Kontrolní hláška – HMAC souhlasí s původním.

Odhalení informace je znázorněno na obrázku 4.8.



Obr. 4.8: Odhalení informace z obrázku.

Různé situace jako stisknutí tlačítka „Dešifrování zprávy“ bez vložení dešifrovacího klíče či vložení chybného dešifrovacího klíče jsou stejně jako v prvním režimu ošetřeny.

5 Ohodnocení zabezpečení

Tato kapitola popisuje jak ohodnocení zabezpečení skrytých informací, tak i varianty zabezpečení, které aplikace umožňuje. V podkapitole 5.1 je vysvětleno, jak byla v aplikaci zajištěna integrita, autentičnost a důvěrnost. Podkapitola 5.2 uvádí vybrané vlastnosti implementované metody a poslední podkapitola 5.3 popisuje úrovně zabezpečení skrývaných informací.

5.1 Zajištění integrity, autentičnosti a důvěrnosti

Aplikace umožňuje volitelně si zvolit, zda danou skrývanou informaci zašifrovat AES šifrou či ne. Dále je možné spočítat HMAC skrývané informace a poté následně porovnat HMAC odkryté informace s původním. V následujícím textu popíšu jak šifru AES, tak HMAC.

5.1.1 AES

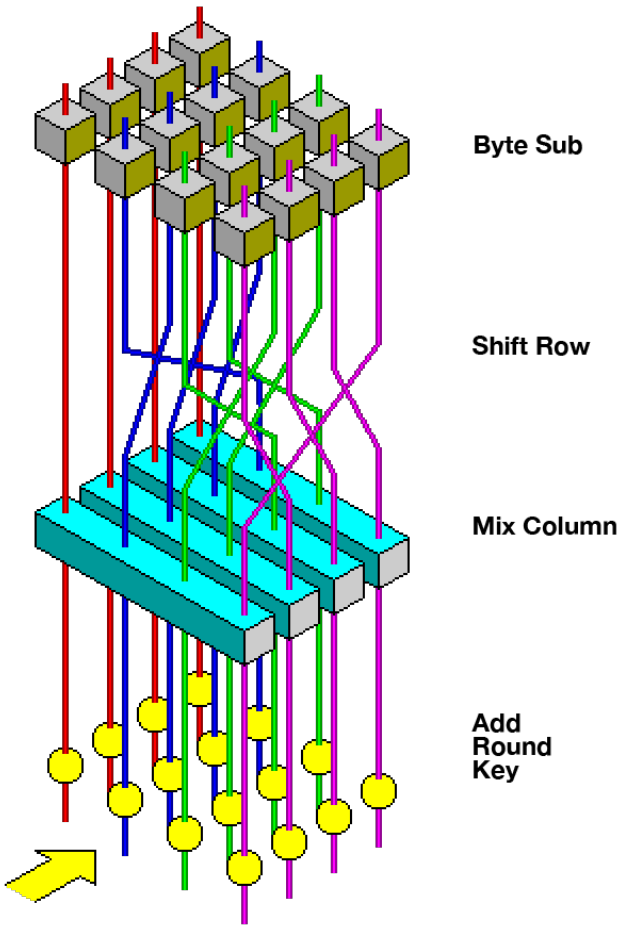
AES je standardizovaný algoritmus, který je využíván k šifrování dat. Patří k symetrickým blokovým šifrám. Data šifruje a dešifruje stejným tajným klíčem. Ta jsou rozdělena do pevně daných bloků o velikosti 128 bitů a následně šifrována pomocí kryptografického klíče, který může mít délku 128, 192 nebo 256 bitů – 256bitový je nejbezpečnější. AES pracuje s maticí bajtů 4×4. Proces šifrování se skládá z několika rund. Každá z nich obsahuje 4 operace viz obrázek 5.1 Počet rund závisí na délce klíče. U 256bitového klíče dochází ke 14 rundám. Díky své bezpečnosti se dnes jedná se nejpoužívanější symetrickou šifru [30, 31].

Pro zvýšení bezpečnosti se používá vybraných módů blokových šifer. Mezi jednotlivými bloky dochází k vytváření vazeb. Způsoby svázání jednotlivých bloků se nazývají operační módy. Výsledkem je, že každý blok je zašifrován jinak. Pro mou implementaci jsem si zvolila AES šifru v módu CBC s klíčem délky 256 bitů. Na obrázku 5.2 je názorně ukázáno šifrování v CBC módu.

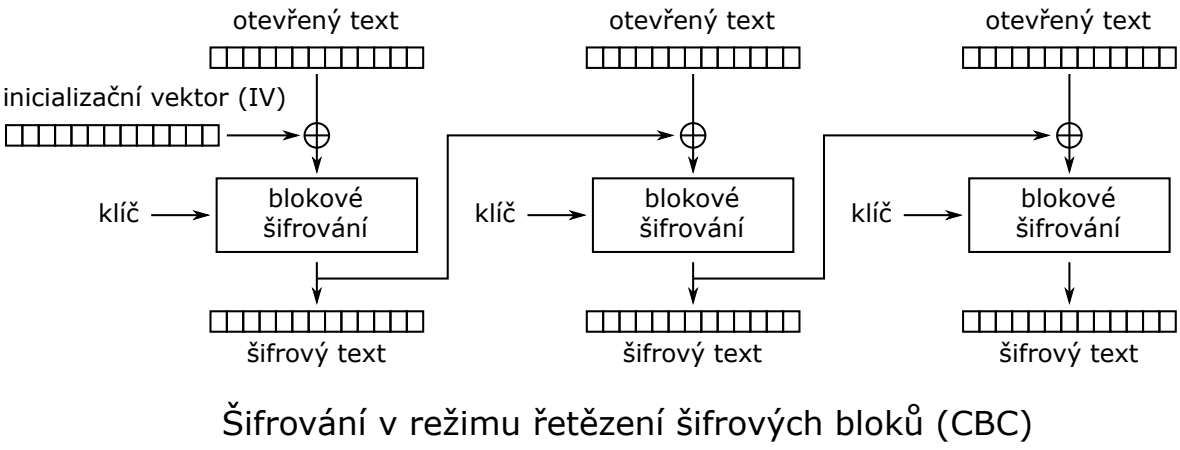
CBC mód používá na začátku inicializační vektor, který je xorován s prvním blokem. Výsledek je poté zašifrován šifrou AES. Každý následující blok je xorován blokem předcházejícím a poté také zašifrován [33].

Pro zašifrování tajné zprávy si v mé aplikaci zvolí uživatel vlastní šifrovací klíč, které se poté zkombinuje pro větší zabezpečení se solí a následně je vytvořen AES šifrovací klíč.

U implementace AES šifry [33, 34] bylo využito následujících knihoven [35, 36, 37]:



Obr. 5.1: Princip rund AES šifry [30].



Obr. 5.2: Mód CBC šifry AES [32].

- **javax.crypto** – tato knihovna poskytuje třídy a rozhraní pro kryptografické operace,
- **javax.crypto.spec** a **java.security.spec** – tyto knihovny poskytují třídy a rozhraní pro specifikace klíčů a specifikace parametrů algoritmů.

5.1.2 HMAC

HMAC je specifický typ autentizačního kódu zprávy, který je počítán s použitím hašovací funkce a tajného šifrovacího klíče. Tento klíč slouží k ověření integrity a autenticity zprávy.

Hašovací funkce slouží k vyjádření reprezentace dat pomocí krátkého řetězce. Požadavky na bezpečnost jsou jednosměrnost(původní data nelze z haše získat), bezkoliznost (vytvoření dvou souborů se stejným hašem je téměř nemožné) a rychlost.

Na vstupu funkce je očekáván sdílený klíč (secret shared key) a text libovolné délky. Výstupem funkce je kód s délkou odpovídající použité hašovací funkci.

Pro vygenerování a ověření kódu se využívá stejného klíče, který je znám jak odesílateli, tak příjemci.

Vlastnosti HMAC (zvláště kryptografická síla) významně závisí na síle použité hašovací funkci a na kvalitě klíče [38, 39].

V mé aplikaci využívám HMAC s hašovací funkcí SHA-256, která patří do skupiny SHA-2 a je považována za jednu z nejbezpečnějších [40]. Bylo využito stejných knihoven jako u AES.

5.2 Vlastnosti metody

Pro ohodnocení implementované metody jsem si vybrala následující tři vlastnosti.

5.2.1 Nepostřehnutelnost

Nepostřehnutelnost je nejdůležitější vlastností metod steganografie. Implementovaná metoda cílí na co největší nepostřehnutelnost pozměněním pouze nejméně významných bitů krycího obrázku. Z toho důvodu je rozdíl mezi původním krycím obrázkem a vytvořeným stego obrázkem téměř neexistující a pouhým okem neviditelný viz obrázek 5.3.

5.2.2 Kapacita

Velmi důležitým kritériem pro ohodnocení metod je kapacita. Udává, jaké množství dat můžeme maximálně do krycího souboru ukrýt. U implementované metody záleží

Obr. 5.3: Porovnání krycího obrázku s vytvořeným stego obrázkem.

na celkovém počtu pixelů obrázku a bitové hloubce viz 3.2.1. Metoda LSB obecně poskytuje velkou kapacitu. Ještě větší kapacity by dosahovala v případě, že by se pro ukrytí zprávy využívaly poslední dva bity.

5.2.3 Robustnost

Robustnost znamená odolnost vůči jakékoli manipulaci. Může jít například o otočení obrázku, změnu velikosti, komprimaci či poslání obrázku přes různé sociální sítě či mail.

Implementovaná metoda je při otočení obrázku schopna odkrýt ukrytou zprávu pouze v případě, že je stego obrázek otočením vrácen na původní pozici. Pokud je otočen o 90 stupňů, 180 či 270 mimo původní pozici, zprávu nelze odkrýt.

Po změně velikosti stego obrázku, ať už zmenšení nebo zvětšení, ukrytou zprávu nelze implementovanou metodou odhalit.

Ukrytá informace se při komprimaci, tedy uložení do archivu, nepoškodí, a proto tajnou zprávu můžeme úspěšně odkrýt.

Po přeposlání steganogramu přes aplikaci WhatsApp dojde ke změně formátu a zprávu poté nelze odkrýt. U přeposlání mailem se steganogram pošle ve stejné kvalitě, a proto zprávu po této operaci odkrýt lze.

5.3 Úrovně zabezpečení skrývané informace

Aplikace umožňuje několik úrovní zabezpečení skrývané informace.

Největšího zabezpečení dosahuje varianta skrytí zašifrované zprávy do krycího obrázku a zároveň vygenerování HMAC. Tato varianta zajišťuje jak důvěrnost, tak i integritu s autentičností.

O něco menšího zabezpečení dosahuje varianta, kdy je tajná zpráva zašifrována a poté skryta do krycího obrázku. Ta zajišťuje důvěrnost ukrývané informace, ale už ne integritu a autentičnost.

Další variantou je ukrytí informace do krycího obrázku bez zašifrování (s vygenerováním HMAC nebo bez). Obecně vzato, pokud je tajná informace zašifrována, ať už je do krycího obrázku skryta či ne, je dosaženo většího zabezpečení, než kdyby byla skrývaná informace ukryta do krycího obrázku bez zašifrování.

U variant bez skrytí informace do obrázku, je nejbezpečnější varianta se zašifrováním a vygenerováním HMAC, o něco méně bezpečné jsou varianty, kdy je tajná zpráva jen zašifrována a kdy je pro ni pouze vygenerován HMAC.

Závěr

V této práci byl čtenář seznámen s vědní disciplínou steganografií, jak v obecném smyslu, tak i v podobě digitální, která využívá pro ukrytí informací například digitální soubory.

V rámci obecné podoby steganografie byly vysvětleny základní principy fungování. Následně byly zmíněny důležité historické okamžiky, které stojí za vývojem steganografie a hlavně přechod do digitálního světa, kde je tato technika bohužel často zneužívána teroristickými organizacemi, crackery a dalšími zločinci. Právě využití steganografie při šíření škodlivého softwaru byla věnována další část mé práce. Využití steganografie při ochraně autorských děl bylo popsáno v následující části. V poslední teoretické části byly popsány a vysvětleny nejznámější typy steganografie a vybrané metody, které se pro tyto typy využívají.

Požadavkem v zadání bylo vytvořit aplikaci využívající vybranou metodu steganografie pro skrytí a odhalení informace. Tato aplikace měla za úkol volitelně zajistit integritu, autentičnost a důvěrnost skryté informace. Těchto cílů bylo dosaženo. Jako metodu určenou pro skrytí a odhalení zprávy jsem si vybrala a implementovala metodu LSB (metodu nejméně významného bitu), pomocí které se bity skrývané zprávy vkládají za nejméně významné bity krycího obrázku. Pro zvýšení zabezpečení informace byl použit šifrovací algoritmus AES a HMAC. Samotná aplikace byla popsána v předposlední části práce. V závěrečné části byl splněn další cíl zadání, a to ohodnocení zabezpečení skrytých informací a úrovní zabezpečení, které aplikace umožňuje.

Steganografie je podle mého názoru velmi důležitý vědní obor, který se bude stále více vyvíjet, už z důvodu častých zneužití steganografických metod při špionážích, kyberútocích a dalších nelegálních aktivitách. Proti takovým situacím je nutné bojovat, a k tomu jsou potřeba znalosti steganografických metod, jejich používání a sledování dalšího vývoje.

Literatura

[1] Johnson, N. F.; Jajodia, S.: *Exploring steganography: Seeing the unseen. Computer.* [online]. Únor 1998, ISSN 1558-0814, doi: 10.1109/MC.1998.4655281. Dostupné z URL: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4655281/>

[2] Nosrati, M.; Karimi, R.; Hariri, M.: *An introduction to steganography methods. World Applied Programming.* [online]. Srpen 2011. Dostupné z URL: <https://www.researchgate.net/publication/308646775_An_introduction_to_steganography_methods/>

[3] Mehta, M.; Shetty, A.: *Digital Watermarking and Steganography, Internation Journal of Engineering Research and Technology (IJERT).* [online]. Říjen 2013, ISSN 2278-0181. Dostupné z URL: <https://www.ijert.org/digital-watermarking-and-steganography/>

[4] Cheddad, A.; Condell, J.; Curran, K.; McKevitt, P.: *Digital image steganography: Survey and analysis of current methods. Signal Processing.* [online]. 2010, ISSN 0165-1684. Dostupné z URL: <https://www.sciencedirect.com/science/article/pii/S0165168409003648/>

[5] Kipper, G.: *Investigator's Guide to Steganography. Auerbach Publications.* 2004, ISBN 0-8493-2433-5.

[6] Djebbar, F.; Beghdad, A.; Abed-Meraim, K.; Hamam, H.: *Comparative Study of Digital Audio Steganography Techniques. EURASIP Journal on Audio, Speech, and Music Processing.* [online]. 2012, doi: 10.1186/1687-4722-2012-25. Dostupné z URL: <https://www.researchgate.net/publication/257879537_Comparative_Study_of_Digital_Audio_Steganography_Techniques/>

[7] Johri, P.; Das, S.; Mishra, A.; Kumar, A.: *Survey on steganography methods (text, image, audio, video, protocol and network steganography). 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom).* [online]. Indie, 2016, ISSN 978-9-3805-4421-2. Dostupné z URL: <https://ieeexplore.ieee.org/document/7724795/>

[8] Johnson, N.; Duric, Z.; Jajodia, S.: *Information Hiding: Steganography and Watermarking-Attacks and Countermeasures. Advances in Information Security.* [online]. Springer US, 2012, ISBN 978-1-4615-4375-6. Dostupné z URL: <https://books.google.com/books?id=29XgBwAAQBAJ/>

[9] Singh, S.: *Kniha kódů a šifer : Tajná komunikace od starého Egypta po kvantovou kryptografii.* Praha: Argo, první vydání, 2003, ISBN 80-7203-499-5.

[10] Mountvernon.org: *Spy techniques of the Revolutionary war.* [online]. Dostupné z URL: <https://www.mountvernon.org/george-washington/the-revolutionary-war/spying-and-espionage/spy-techniques-of-the-revolutionary-war/>

[11] Mountvernon.org: *How was invisible ink used by Washington?.* [online]. Dostupné z URL: <https://www.mountvernon.org/education/online-activities-for-kids-2/how-to-make-invisible-ink//>

[12] Zielińska, E.; Mazurczyk, W.; Szczypiorski, K.: *Trends in steganography. Communications of the ACM.* [online]. Březen 2014, doi: 10.1145/2566590.2566610. Dostupné z URL: <https://www.researchgate.net/publication/262248599_Trends_in_steganography/>

[13] Cs.wikipedia.org: *Temný web – Wikipedie.* [online]. 2020. Dostupné z URL: <https://cs.wikipedia.org/wiki/Temný_web>

[14] Nag, A.; Singh, J.; Khan, S.; Ghosh, S.; Biswas, S.; Sarkar, D.; Sarkar, P.: *A Weighted Location Based LSB Image Steganography Technique.* [online]. Červenec 2011, doi: 10.1007/978-3-642-22714-1. Dostupné z URL: <https://www.researchgate.net/publication/220790121_A_Weighted_Location_Based_LSB_Image_Steganography_Technique/>

[15] Welivesecurity.com: *Readers of popular websites targeted by stealthy Stegano exploit kit hiding in pixels of malicious ads.* [online]. Prosinec 2016. Dostupné z URL: <https://www.welivesecurity.com/2016/12/06/readers-popular-websites-targeted-stealthy-stegano-exploit-kit-hiding-pixels-malicious-ads/>

[16] Root.cz: *Postřehy z bezpečnosti: reklama na skrytý malware.* [online]. Prosinec 2016. Dostupné z URL:

<https://www.root.cz/clanky/postrehy-z-bezpecnosti-reklama-na-skryty-malware/>

[17] Kaspersky.com: *Industrial espionage in action: a new toolset is being deployed against industrial holdings.* [online]. Říjen 2020. Dostupné z URL: <https://www.kaspersky.com/about/press-releases/2020_industrial-espionage-in-action-a-new-toolset-is-being-deployed-against-industrial-holdings/>

[18] Securityboulevard.com: *New MontysThree Toolset Used in Targeted Industrial Espionage Attacks.* [online]. Říjen 2020. Dostupné z URL: <https://securityboulevard.com/2020/10/new-montysthree-toolset-used-in-targeted-industrial-espionage-attacks/>

[19] Usa.kaspersky.com: *Infamous hacker-for-hire group DeathStalker hits the Americas and Europe with new PowerPepper malware.* [online]. Prosinec 2020. Dostupné z URL: <https://usa.kaspersky.com/about/press-releases/2020_infamous-hacker-for-hire-group-death-stalker-hits-the-americas-and-europe-with-new-power-pepper-malware/>

[20] Arsenova, E.: *Technical Aspects of Digital Rights Management.* [online]. Německo, 2008. Dostupné z URL: <http://www.hit.bme.hu/~jakab/edu/litr/DRM/old/Techn_Asp_of_DRM.pdf/>

[21] Obimbo, Ch.; Salami, B.: *Using Digital Watermarking for Copyright Protection, Watermarking - Volume 2, Dr. Mithun Das Gupta (Ed.).* [online]. 2012, ISBN: 978-953-51-0619-7. Dostupné z URL: <https://www.intechopen.com/books/watermarking-volume-2/using-digital-watermarking-for-copyright-protection/>

[22] Thampi, S.: *Information Hiding Techniques: A Tutorial Review.* [online]. Indie, 2008. Dostupné z URL: <https://arxiv.org/ftp/arxiv/papers/0802/0802.3746.pdf/>

[23] Morkel, T.; Eloff J. H. P.; Olivier, M. S.: *An Overview of Image Steganography. Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005).* [online]. Jižní Afrika, Červen 2005. Dostupné z URL: <https://digifors.cs.up.ac.za/issa/2005/Proceedings/Full/098_Article.pdf/>

[24] Kolarčík, T.: *Digitální obrazová steganografie.* [online]. Bakalářská práce, Vysoké učení technické, Fakulta informatiky, Brno, 2019. Dostupné z URL: <https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=197274/>

[25] Codementor.io: *Everything that you need to know about Image Steganography.* [online]. Leden 2020. Dostupné z URL: <https://www.codementor.io/@arpitbhayani/internals-of-image-steganography-12qsxcxjsh/>

[26] Da-Chun, W.; Wen-Hsiang, T.: *A steganographic method for images by pixel value differncing. Pattern Recognition Letters.* [online]. Červenec 2003, doi: 10.1016/S0167-8655(02)00402-6. Dostupné z URL: <https://www.researchgate.net/publication/223256802_A_steganographic_method_for_images_by_pixel_value_differncing/>

[27] Megha, M.: *Methods of Audio Steganography. International Journal of Engineering and Management Research.* [online]. Červen 2014, ISSN 2250-0758. Dostupné z URL: <https://www.ijemr.net/DOC/MethodsOfAudioSteganography(154-156)427829c3-2546-45d2-9f3d-ca625c6f8605.pdf/>

[28] Singh, H.; Singh, P.; Saroha, K.: *A Survey on Text Based Steganography. Proceedings of the 3rd National Conference.* [online]. Indie, 2009. Dostupné z URL: <https://www.researchgate.net/publication/267920012_A_Survey_on_Text_Based_Steganography/>

[29] Docs.oracle.com: *Package javax.swing.* [online]. Dostupné z URL: <https://docs.oracle.com/javase/7/docs/api/javax/swing/package-summary.html/>

[30] En.wikipedia.org: *Advanced Encryption Standard.* [online]. 2021. Dostupné z URL: <https://en.wikipedia.org/wiki/Advanced_Encryption_Standard/>

[31] Cs.wizcase.com: *Kompletní návod na standard pokročilého šifrování (AES).* [online]. Říjen 2018. Dostupné z URL: <https://cs.wizcase.com/blog/kompletni-navod-na-standard-pokrocileho-sifrovani-aes/>

[32] Cs.wikipedia.org: *Provozní režim blokových šifer.* [online]. 2021. Dostupné z URL:
<https://cs.wikipedia.org/wiki/Provozní_režim_blokových_šifer>

[33] Baeldung.com: *Java AES Encryption and Decryption.* [online]. Indie, 2009. Dostupné z URL:
<https://www.baeldung.com/java-aes-encryption-decryption/>

[34] Itnetwork.cz: *Šifrování v Javě pomocí algoritmu AES 256.* [online]. 2013. Dostupné z URL:
<https://www.itnetwork.cz/java/oop/zdrojove-kody/tutorial-java-sifrovani-algoritmus-aes-256/>

[35] Docs.oracle.com: *Package java.security.spec.* [online]. Dostupné z URL:
<https://docs.oracle.com/javase/7/docs/api/java/security/spec/package-summary.html/>

[36] Docs.oracle.com: *Package javax.crypto.spec.* [online]. Dostupné z URL:
<https://docs.oracle.com/javase/7/docs/api/javax/crypto/spec/package-summary.html/>

[37] Docs.oracle.com: *Package javax.crypto.* [online]. Dostupné z URL:
<https://docs.oracle.com/javase/7/docs/api/javax/crypto/package-summary.html/>

[38] Cleverandsmart.cz: *Základy kryptografie pro manažery: HMAC.* [online]. Srpen 2011. Dostupné z URL:
<https://www.cleverandsmart.cz/zaklady-kryptografie-pro-manazery-hmac/>

[39] Freecodecamp.org.cz: *MD5 vs SHA-1 vs SHA-2 - Which is the Most Secure Encryption Hash and How to Check Them.* [online]. Březen 2020. Dostupné z URL:
<https://www.freecodecamp.org/news/md5-vs-sha-1-vs-sha-2-which-is-the-most-secure-encryption-hash-and-how-to-check-them/>

[40] Freecodecamp.org.cz: *HmacSHA256 Signature in Java.* [online]. Červenec 2020. Dostupné z URL:
<https://www.javacodemonk.com/create-hmacsha256-signature-in-java-3421c36d/>

Seznam symbolů a zkratek

AES Advanced Encryption Standard – symetrický algoritmus používaný k šifrování dat

ASCII American Standard Code for Information Interchange – kódovací tabulka obsahující znaky abecedy a další znaky používající se ve výpočetní technice

CBC Cipher Block Chaining – operační mód šifry AES

CVE Common Vulnerabilities and Exposures – seznam standardizovaných názvů pro zranitelnosti a další ohrožení informační bezpečnosti

DCT Discrete Cosine Transform – diskrétní cosinová transformace

DNS Domain Name System – protokol pro převod doménových jmen a IP adres

DWT Discrete Wavelet Transform – diskrétní vlnková transformace

GUI Graphical User Interface – grafické uživatelské rozhraní

HMAC Keyed-hash Message Authentication Code – druh autentizačního kódu zprávy, který je spočítán použitím kryptografické hašovací funkce v kombinaci s tajným šifrovacím klíčem.

HTML Hypertext Markup Language – značkovací jazyk používaný pro tvorbu webových stránek

HTTP Hypertext Transfer Protocol – internetový protokol určený pro komunikaci s WWW servery

HTTPS Hypertext Transfer Protocol Secure – protokol umožňující zabezpečenou komunikaci v počítačové síti

I2P Invisible Internet Projekt – název překryvné počítačové sítě

IP Internet Protocol – protokol síťové vrstvy

LSB Least Significant Bit – nejméně významný bit

RGB Red Green Blue – aditivní způsob míchání barev složený ze tří složek (červená, zelená, modrá)

RGBA Red Green Blue Alpha – barevný model RGB rozšířený o alfa kanál určující průhlednost konkrétního pixelu

VoIP Voice over Internet Protocol – internetová telefonie

XML Extensible Markup Language – značkovací jazyk